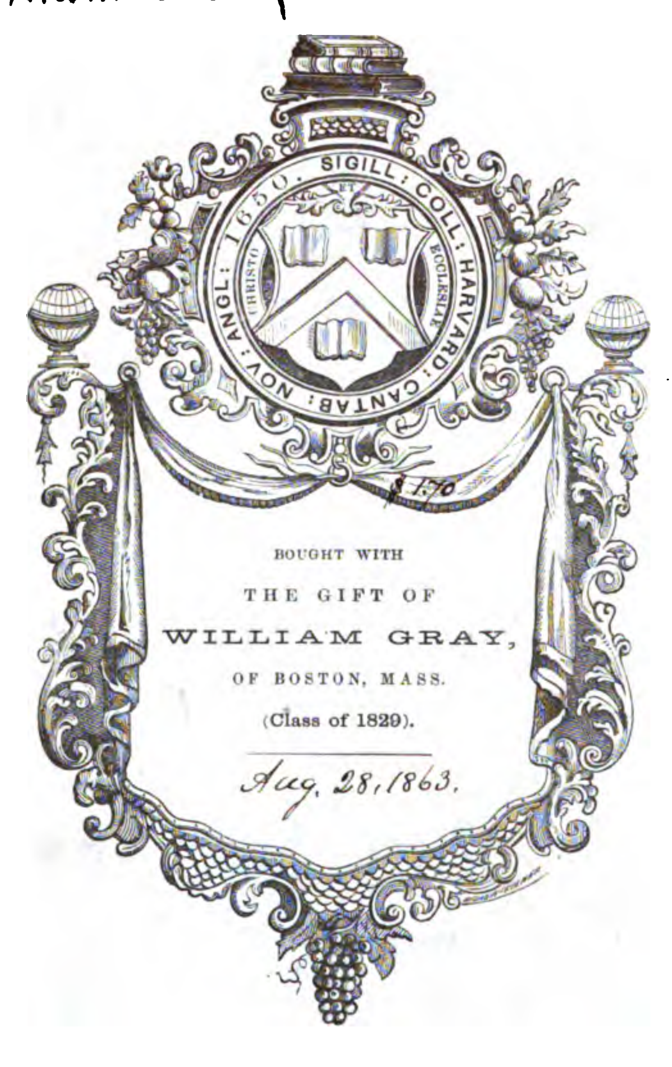
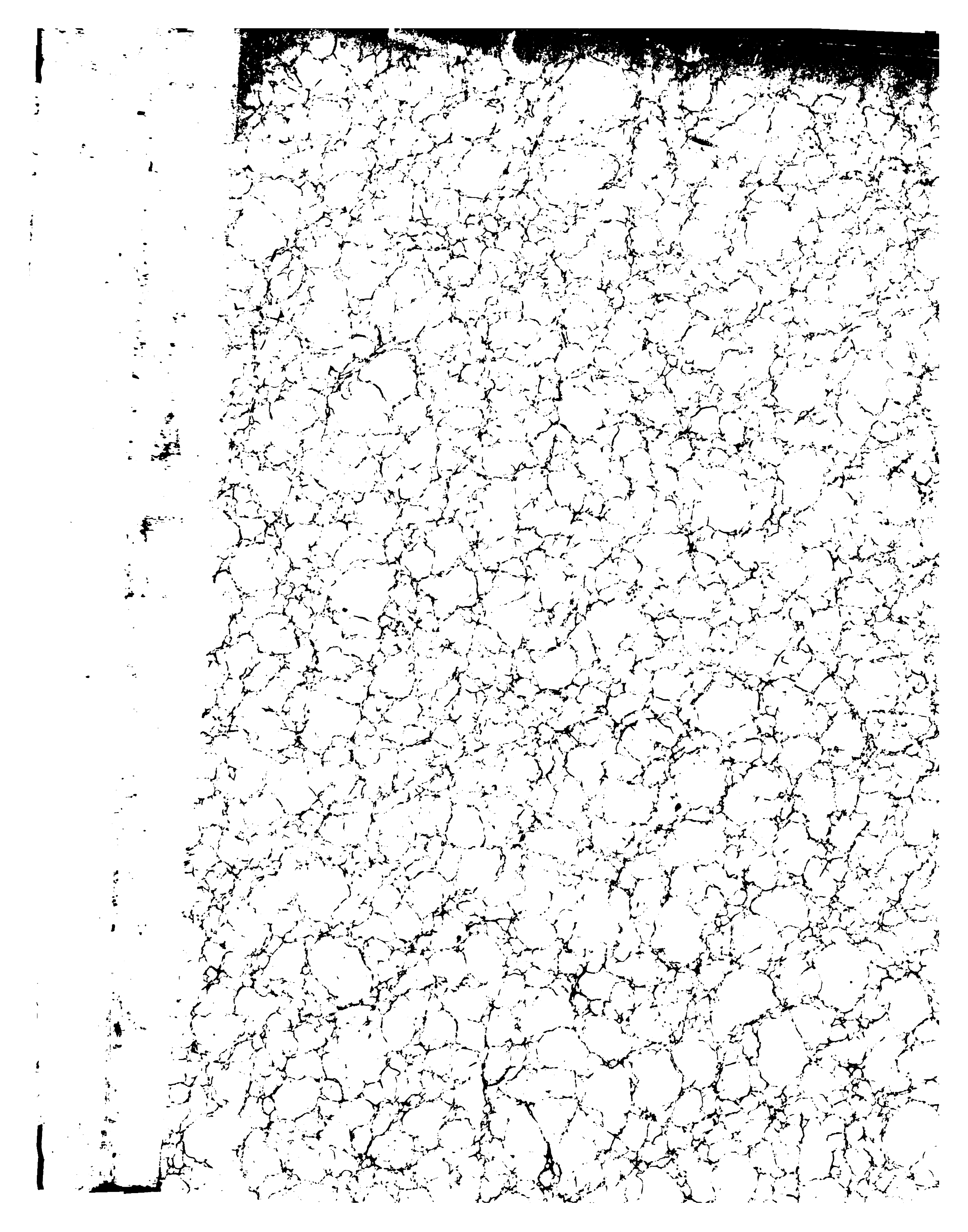
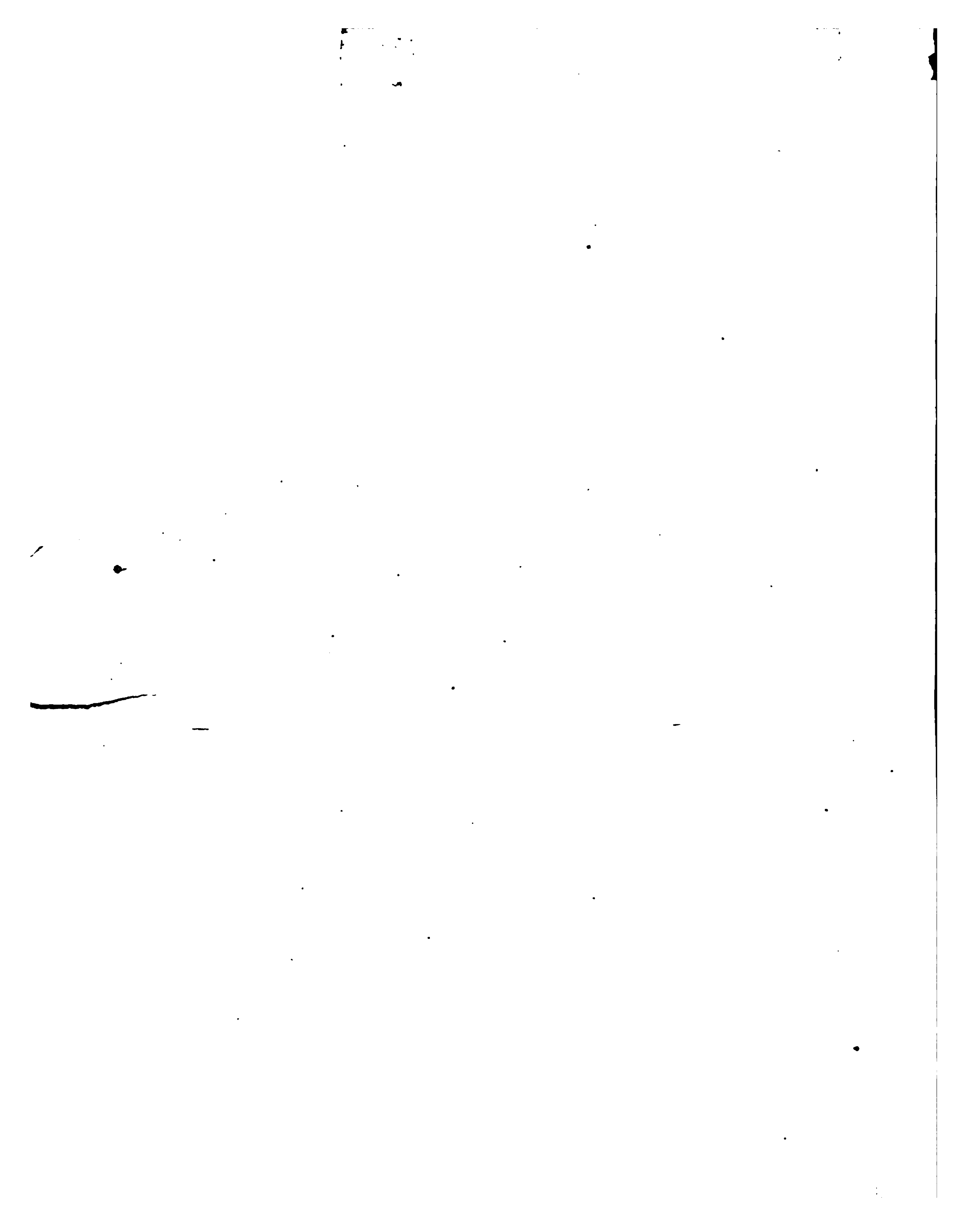


QA
241
K8




SIGILL: COLL: HARVARD: CANTAB: NOV: ANGL: 1650.
CHRISTO ET ECCLESIAE
$1.70
BOUGHT WITH
THE GIFT OF
WILLIAM GRAY,
OF BOSTON, MASS.
(Class of 1829).
Aug. 28, 1863.





Über

die allgemeinen Reciprocitätsgesetze

unter

den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist.

Von

Ernst Eduard
E. E. KUMMER.

Aus den Abhandlungen der Königl. Akademie der Wissenschaften zu Berlin 1859.

Berlin.

Gedruckt in der Druckerei der Königl. Akademie
der Wissenschaften.

1859.

In Commission von F. Dümmlers Verlags-Buchhandlung.

Gelesen in der Akademie der Wissenschaften am 18. Februar 1858 und am 5. Mai 1859.
Die Seitenzahl bezeichnet die laufende Pagina des Jahrgangs 1859 in den Abhandlungen der mathematischen Klasse der Königl. Akademie der Wissenschaften.

Die Reciprocitätsgesetze, welche unter den Resten und Nichtresten der Potenzen Statt haben, bilden gewissermaafsen den Schlufsstein der Lehre von den Potenzresten und eröffnen zugleich den Weg für weitere und tiefer liegende arithmetische Untersuchungen. Sie sind in diesen beiden Beziehungen für die Zahlentheorie von grofser Wichtigkeit, aber eine noch höhere Bedeutung haben sie in der geschichtlichen Entwickelung dieser mathematischen Disciplin dadurch erlangt, dafs die Beweise derselben, so weit sie überhaupt gefunden sind, fast durchgängig aus neuen, bis dahin noch unerforschten Gebieten haben geschöpft werden müssen, welche so der Wissenschaft aufgeschlossen worden sind. Wegen dieser Schwierigkeit der Beweise ist man in der Erkenntnifs der Reciprocitätsgesetze bisher nicht viel über die quadratischen, kubischen und biquadratischen hinausgekommen, obgleich mehrere der ausgezeichnetsten Mathematiker der neueren Zeit sie zum Gegenstande ihrer Forschungen gemacht haben.

Euler hat das Verdienst, das Reciprocitätsgesetz für quadratische Reste zuerst bemerkt zu haben, m. s. dessen *Commentationes arithmeticae collectae* Bd. 1, pg. 486, aber man kennt keinen Versuch, den er gemacht hätte dasselbe zu beweisen. Hierauf hat Legendre, von Euler unabhängig, dieses Gesetz ebenfalls gefunden, und weil er dessen grofse Wichtigkeit erkannte, einen sehr sinnreichen Beweis desselben aufgestellt, welcher nur in so fern unvollständig ist, als er voraussetzt, dafs zu einer jeden Primzahl von der Form $4n+1$ eine Primzahl der Form $4n+3$ gefunden werden

kann, in Beziehung auf welche jene quadratischer Nichtrest ist, welches Postulat leicht von dem allgemeineren Satze abhängig gemacht wird, dafs jede arithmetische Reihe, in welcher nicht alle Glieder einen gemeinschaftlichen Faktor haben, nothwendig Primzahlen enthalten mufs. Um diesen Mangel des Legendreschen Beweises zu heben, hat später Hr. Dirichlet diese Eigenschaft der arithmetischen Reihen streng bewiesen, und zwar durch die neuen, überaus fruchtbaren Methoden, durch deren Hülfe er auch die Klassenanzahl der quadratischen Formen gefunden hat. Diese berühmten Arbeiten des Hrn. Dirichlet können daher als solche betrachtet werden, welche der Beschäftigung mit den Reciprocitätsgesetzen ihre Entstehung verdanken.

Den ersten vollständigen und strengen Beweis des quadratischen Reciprocitätsgesetzes hat Gaufs in seinen *Disquisitiones arithmeticae* pg. 124, sq. gegeben, indem er gezeigt hat, dafs, wenn dieses Gesetz für alle Primzahlen bis zu einer bestimmten Gränze hin richtig ist, dasselbe auch richtig bleibt, wenn diese Gränze so weit erweitert wird, dafs sie eine Primzahl mehr umfafst, woraus nach dem bekannten Schlusse der Induktionsbeweise die Allgemeingültigkeit desselben folgt. Dieser Beweis, welcher vor allen übrigen sich dadurch auszeichnet, dafs er keine, dem Gebiete der Congruenzen zweiten Grades fremden Hülfsmittel braucht, ist später von Hrn. Dirichlet in einfacherer Weise dargestellt worden in Crelle's Journal, Bd. 47, pg. 139.

Der zweite Beweis des *theorema fundamentale*, wie Gaufs dieses Reciprocitätsgesetz der quadratischen Reste bezeichnet, findet sich ebenfalls in den *Disquisitiones arithmeticae*, pg. 414, sq., wo er aus der Theorie der quadratischen Formen abgeleitet wird. Die Grundgedanken desselben werde ich weiter unten genauer zu entwickeln Gelegenheit nehmen, da es diejenigen sind, welche ich für den ersten Beweis des allgemeinen Reciprocitätsgesetzes in Anwendung gebracht habe, den ich in der gegenwärtigen Abhandlung geben will.

Aufser den beiden, in den *Disquisitiones arithmeticae* enthaltenen Beweisen hat Gaufs später noch vier verschiedene Beweise desselben Satzes in den Commentarien der Göttinger Akademie gegeben. Zwei von diesen, nämlich der als dritter und der als fünfter von Gaufs bezeichnete, sind beinahe eben so elementar, als der erste Beweis, da sie nur in so fern das Gebiet der Congruenzen zweiten Grades verlassen, als ein Satz über die reinen

Congruenzen höherer Grade hinzugezogen wird. Beide Beweise stützen sich auch auf einen und denselben, nicht schwer zu beweisenden Satz, welcher in der Abzählung der kleinsten positiven Reste einer arithmetischen Reihe, die gröfser als die Hälfte des Moduls sind, ein Kriterium dafür giebt, ob eine gegebene Zahl quadratischer Rest oder Nichtrest dieses Moduls ist. Der Unterschied derselben liegt hauptsächlich nur in der Art der Abzählung dieser Reste, welche in dem einen Beweise für sich selbst betrachtet, in dem anderen aber durch die gröfsten Ganzen ausgedrückt werden, welche in gewissen gebrochenen Zahlen enthalten sind. Als eine Modification dieser Gaufsischen Beweise ist auch derjenige anzusehen, welchen Eisenstein in Crelle's Journal, Bd. 28, pg. 246, gegeben hat. Dieser Beweis unterscheidet sich nämlich von dem dritten Gaufsischen nur darin, dafs geometrische Anschauungen zu Hülfe genommen, und die in den Brüchen enthaltenen gröfsten Ganzen durch die Anzahl der in bestimmten Gränzen liegenden Gitterpunkte eines Netzes dargestellt werden.

Die anderen beiden Gaufsischen Beweise haben ihre Quelle in der Theorie der Kreistheilung. Diese zeigt, wie die Quadratwurzel einer jeden gegebenen Zahl durch Wurzeln der Einheit in ganzer rationaler Form dargestellt werden kann, wobei nur der eine Punkt unentschieden bleibt: ob diese Darstellung den Werth der Quadratwurzel mit dem positiven oder mit dem negativen Vorzeichen giebt. Die Bestimmung dieses Vorzeichens ist der hauptsächlichste Gegenstand der Gaufsischen Abhandlung, welche den vierten Beweis des quadratischen Reciprocitätsgesetzes enthält, und den Titel *Summatio quarundam serierum singularium* führt. Dieselbe, sowohl durch die Einfachheit des für Primzahlen und für zusammengesetzte Zahlen gleichmäfsig geltenden Resultats, als auch durch die Schwierigkeit des Beweises interessante Vorzeichenbestimmung, nebst dem darauf gegründeten Beweise des Reciprocitätsgesetzes, ist später von Hrn. Dirichlet, in einer vor der Akademie im Jahre 1835 vorgetragenen Abhandlung, nach einer anderen Methode, mit Anwendung bestimmter Integrale, ausgeführt worden.

Der sechste Gaufsische Beweis, welcher auch auf der Kreistheilung beruht, uud zwar auf demselben Ausdrucke der Quadratwurzel aus p durch $p$te Wurzeln der Einheit, unterscheidet sich wesentlich dadurch von dem anderen, dafs er die Bestimmung des Vorzeichens der Quadratwurzel nicht erfordert. Der eigentliche Kern dieses Beweises wird bei Gaufs dadurch

etwas verhüllt, dafs anstatt der $p$ten Wurzel der Einheit eine unbestimmte Variable x angewendet wird, was zur Folge hat, dafs Congruenzen unter ganzen rationalen Funktionen von x nach dem Modul $1+x+x^2+\ldots+x^{p-1}$ angewendet werden müssen, anstatt deren man nur einfache Gleichungen erhält, wenn dem x der specielle Werth einer primitiven $p$ten Wurzel der Einheit gegeben wird. Diese Vereinfachung des sechsten Gaufsischen Beweises hat zuerst Jacobi ausgeführt und im Jahre 1827 an Legendre brieflich mitgetheilt, welcher sie im Jahre 1830 in die dritte Ausgabe seiner théorie des nombres aufgenommen hat. Mit dieser Jacobischen Darstellung des Gaufsischen Beweises stimmt auch ein von Cauchy in Férussac bulletin im Jahre 1829 gegebener Beweis des Reciprocitätsgesetzes im Wesentlichen überein. Eisenstein, welchem Jacobi's und Cauchy's Arbeiten über diesen Gegenstand unbekannt geblieben waren, hat denselben Beweis im Jahre 1844 in Crelle's Journal, Bd. 28, pag. 41, reproducirt.

Die aufserdem noch zu erwähnenden Beweise des quadratischen Reciprocitätsgesetzes hängen alle mit der Theorie der Kreistheilung zusammen. Am nächsten steht den von Jacobi und Cauchy gegebenen Beweisen derjenige, welchen Hr. Liouville im 12ten Bande seines Journal's, pg. 95, aufgestellt hat, dessen Unterschied von jenen hauptsächlich nur darin liegt, dafs Hr. Liouville nicht den Ausdruck der Quadratwurzel aus p durch eine Summe von $p$ten Wurzeln der Einheit, sondern den Ausdruck als Produkt von Differenzen dieser Einheitswurzeln anwendet, welcher, wenn man von den fertigen Resultaten der Kreistheilung keinen Gebrauch machen will, viel leichter unmittelbar herzustellen ist, und darum einen Vorzug vor jenem hat. Der Beweis von Hrn. Lebesgue, in Liouville's Journal, Bd. 3, pag. 134, beruht auf der vollständigen Potenzerhebung des Ausdrucks der Quadratwurzel aus p durch die Einheitswurzeln, wodurch die $\frac{1}{2}(q-1)$te Potenz von p gewonnen wird, ohne dafs die Vielfachen von q weggelassen werden. Die Coefficienten dieser Entwickelung, welche nur drei verschiedene Zahlen sind, werden in bekannter Weise durch die Anzahl der Auflösungen gewisser Congruenzen definirt, und aus dem so bestimmten Ausdrucke der $\frac{1}{2}(q-1)$ten Potenz von p wird das Reciprocitätsgesetz für die beiden Primzahlen p und q ohne Schwierigkeit erschlossen. An diesen Beweis von Hrn. Lebesgue schliefst sich der von Eisenstein, in Crelle's Journal, Bd. 27, pag. 322, gegebene Beweis sehr genau an, obgleich er

scheinbar von ganz anderen Prinzipien ausgeht. Eisenstein gebraucht in demselben gewisse Zahlenausdrücke, welche auf combinatorischem Wege aus den bekannten Legendreschen Zeichen, deren Werthe nur $+1$ und -1 sind, je nachdem eine Zahl Rest oder Nichtrest der anderen ist, zusammengesetzt werden, und er stellt durch diese die $\frac{1}{2}(q-1)$te Potenz von p so dar, dafs durch Weglassung der Vielfachen von q das Reciprocitätsgesetz gewonnen wird. Betrachtet man aber diese Eisensteinschen Zahlenausdrücke näher, so bemerkt man leicht ihren Ursprung aus der Kreistheilung, welchen Eisenstein selbst verschwiegen hat, und man erkennt, dafs sie nichts anderes sind, als die Coefficienten der Entwickelung einer Potenz des Ausdrucks von $\sqrt{p}$ durch die $p$ten Wurzeln der Einheit, und dafs sie mit den von Hrn. Lebesgue durch die Anzahl der Auflösungen gewisser Congruenzen definirten Zahlen wesentlich übereinstimmen. Dieses hat auch Hr. Lebesgue, in Liouville's Journal, Bd. 12, pag. 457, nachgewiesen.

Für einen der schönsten Beweise dieses von den ausgezeichnetsten Mathematikern viel bewiesenen Theorems wird aber derjenige mit Recht gehalten, welchen Eisenstein in Crelle's Journal, Bd. 29, pag. 177, gegeben hat. In diesem wird das Legendresche Zeichen $\left(\frac{p}{q}\right)$ durch Kreisfunktionen so ausgedrückt, dafs bei der Vertauschung von p und q dieser Ausdruck, bis auf eine leicht zu bestimmende Änderung im Vorzeichen, ungeändert bleibt. Dieser Beweis hängt in so fern ebenfalls mit der Theorie der Kreistheilung zusammen, als der Ausdruck des $\left(\frac{p}{q}\right)$ nur die Sinus der Vielfachen von $\frac{2\pi}{p}$ enthält, welche mit den $p$ten Wurzeln der Einheit ganz auf derselben Stufe stehen, auch ist dieser Ausdruck mit dem von Hrn. Liouville in seinem Beweise angewendeten Produktausdrucke der Quadratwurzel aus p nahe verwandt. Wenn dieser Eisensteinsche Beweis schon wegen seiner vorzüglichen Eleganz beachtenswerth ist, so wird der Werth desselben noch dadurch erhöht, dafs er, wie Eisenstein selbst gezeigt hat, ohne besondere Schwierigkeit auch auf die biquadratischen und die kubischen Reciprocitätsgesetze angewendet werden kann, wenn anstatt der Kreisfunktionen elliptische Funktionen mit bestimmten Moduln angewendet werden.

Was nun in dem Gebiete der Reciprocitätsgesetze für die Reste und Nichtreste höherer Potenzen bisher geleistet worden ist, beschränkt sich zwar hauptsächlich nur auf die vollständigen Beweise dieser Gesetze für die

biquadratischen und die kubischen Reste und Nichtreste und darüber hinaus nur auf gewisse sehr specielle Fälle; es ist aber grade dieses für die ganze weitere Entwickelung der Zahlentheorie von den bedeutendsten Folgen gewesen, weil dadurch das Gebiet dieser mathematischen Disciplin unendlichfach erweitert worden ist, nach Gaufs eigenen Worten: *ut campus Arithmeticae sublimioris infinities quasi promoveatur.* Der eben so einfache als vielumfassende Gedanke dieser Erweiterung der Zahlentheorie, nämlich die Einführung complexer ganzer Zahlen, welche unter denselben Gesichtspunkten betrachtet werden können, als die gewöhnlichen ganzen Zahlen, ist zuerst in der im Jahre 1828 erschienenen, aber der Göttinger Akademie schon im Jahre 1825 übergebenen Abhandlung von Gaufs, über die biquadratischen Reste, niedergelegt, und in einer zweiten Abhandlung über denselben Gegenstand vom Jahre 1832 weiter ausgeführt. Nach Jacobi's Meinung ist dieser Gedanke nicht aus dem Gebiete der Arithmetik allein erwachsen, sondern unter Mitwirkung der Theorie der elliptischen Funktionen, namentlich der lemniskatischen, für die eine complexe Multiplikation mit Zahlen von der Form $a+b\sqrt{-1}$ und die entsprechende Division Statt hat, welche Gaufs für sich schon über ein Vierteljahrhundert eher gekannt hat, als sie durch die Arbeiten von Abel und Jacobi ein Allgemeingut der Wissenschaft geworden ist. Zwar ist in der Gaufsischen Darstellung des Gedankens der complexen Zahlen keine Spur dieses von Jacobi vermutheten Ursprungs zu finden; da aber Gaufs in seinen Ahandlungen mehr darauf ausging, die mathematischen Wahrheiten kunstgerecht aufzubauen, als sie genetisch zu entwickeln, und da er nach seinem eigenen Ausdrucke das Gerüst abtrug, wenn der Bau vollendet war, so läfst sich schwer entscheiden, ob wirklich die Lemniskatenfunktionen mit zu den Balken des Gerüstes gehört haben, mit dessen Hülfe er dieses unvergängliche Werk errichtet hat. In der Theorie der biquadratischen Reste erscheint die Einführung der complexen Zahlen von der Form $a+b\sqrt{-1}$ dadurch motivirt, dafs die biquadratischen Reciprocitätsgesetze für gewöhnliche Primzahlen sehr complicirt sind, namentlich für die Primzahlen von der Form $4n+1$, welche sich als Summen zweier Quadratzahlen darstellen lassen, dafs diese Reciprocitätsgesetze aber die einfachste Form annehmen, wenn man die gewöhnlichen Primzahlen von der Form $p=a^2+b^2$ in die imaginären Faktoren $a+b\sqrt{-1}$ und $a-b\sqrt{-1}$ zerlegt, und unter diesen als den für die vor-

liegende Frage wahren Primzahlen die Reciprocitätsgesetze aufstellt. Dieses neue Princip ist es, welches die genannten beiden Gaufsischen Abhandlungen zu Dokumenten einer bedeutenden Epoche in der geschichtlichen Entwickelung der Zahlentheorie erhebt, welche auch auf die verwandten mathematischen Disciplinen einen grofsen Einflufs ausgeübt hat; die in den Abhandlungen enthaltenen neuen Sätze über biquadratische Reste treten dagegen in den Hintergrund. Gaufs hat nämlich in denselben nur diejenigen Sätze vollständig bewiesen, welche als die Ergänzungssätze zu dem biquadratischen Reciprocitätsgesetze bezeichnet werden müssen, da sie grade nur die biquadratischen Charaktere derjenigen Zahlen geben, auf welche der allgemeine Ausdruck dieses Gesetzes sich nicht erstreckt. Das vollständige Reciprocitätsgesetz für die Reste der vierten Potenzen hat er nur aufgestellt, und sein Beweis desselben, welcher in der dritten Abhandlung folgen sollte, ist niemals erschienen.

Als die erste der beiden genannten Gaufsischen Abhandlungen noch nicht erschienen war, sondern nur eine vorläufige Ankündigung derselben in den Göttinger gelehrten Anzeigen, aus welcher nicht mehr zu erfahren war, als dafs die Lösung der Frage: ob eine Zahl biquadratischer Rest einer gegebenen Primzahl ist, oder nicht, von den Zahlenwerthen der Unbestimmten gewisser quadratischer Formen abhängig sei, in welche der Modul gesetzt werden kann, veröffentlichte Hr. Dirichlet eine Abhandlung über die biquadratischen Reste, in Crelle's Journal, Bd. 3, pag. 35. In dieser ist er, ohne von dem noch nicht bekannten neuen Gaufsischen Prinzipe der complexen Zahlen Gebrauch machen zu können, durch blofse Anwendung der Theorie der quadratischen Formen und Reste schon sehr tief in die Theorie der biquadratischen Reste eingedrungen, ohne jedoch das Reciprocitätsgesetz derselben finden zu können.

In demselben Jahre 1827 fand Jacobi in der Theorie der Kreistheilung, die er bedeutend vereinfacht und weiter ausgebildet hatte, eine reiche Quelle für die Reciprocitätsgesetze der Potenzreste, aus welcher er nicht nur den oben bereits erwähnten Beweis des quadratischen Reciprocitätsgesetzes ableiten konnte, sondern auch die in Crelle's Journal, Bd. 2, pg. 66, von ihm aufgestellten Sätze über kubische Reste, aus welcher er auch einige Zeit später, durch Anwendung des neuen Gaufsischen Prinzip's, die vollständigen Reciprocitätsgesetze für die kubischen und die biquadratischen

Reste in ihrer einfachsten Gestalt hergeleitet und bewiesen hat. Die vollständige Entwickelung dieser Sätze hat Jacobi aber nur in seinen Vorlesungen über Zahlentheorie, in denen die Lehre von der Kreistheilung den eigentlichen Kern bildete, seinen Zuhörern in Königsberg mitgetheilt, durch deren Hefte sie sodann weiter verbreitet worden sind. Aufserdem hat Jacobi der hiesigen Akademie zwei Mittheilungen darüber in den Jahren 1837 und 1839 gemacht, welche in den Monatsberichten veröffentlicht sind. In der letzteren dieser Mittheilungen spricht er auch die Erwartung aus, dafs er aus derselben Quelle eben so die Reciprocitätsgesetze für die fünften und achten Potenzen werde ableiten können, eine Erwartung, welche nicht erfüllt werden konnte, wie bald näher gezeigt werden soll.

Aufser Gaufs, Jacobi und Dirichlet hat nur noch Eisenstein in diesem Gebiete der kubischen und biquadratischen Reste selbständig und mit Erfolg gearbeitet. Seine ersten Beweise, des kubischen Reciprocitätsgesetzes, in Crelle's Journal, Bd. 27, pag. 289, und des biquadratischen, ebendaselbst Bd. 28, pag. 53, sind zwar nur ganz dieselben, welche Jacobi mehr als zehn Jahre früher gefunden hatte, auch ist der Beweis des biquadratischen Reciprocitätsgesetzes in Crelle's Journal, Bd. 28, p. 233, welcher dem oben besprochenen ebendaselbst, Bd. 27, pag. 322, entspricht, und ebenso wie dieser seine Abstammung aus der Kreistheilung verbirgt, zwar scharfsinnig, wie alle Arbeiten Eisenstein's, aber doch mehr nur scheinbar als wirklich originell; aber Eisenstein ist bei diesen nicht stehen geblieben, sondern hat bald darauf neue Beweise dieser Gesetze gegeben, welche mit zu seinen vorzüglichsten Leistungen zu rechnen sind und mit Recht die Bewunderung der ersten Mathematiker erregt haben. Es sind diefs die schon oben beiläufig erwähnten Beweise, welche die quadratischen, kubischen und biquadratischen Reciprocitätsgesetze in ähnlicher Weise umfassen, in der Art, dafs zu dem Beweise des kubischen die elliptischen Funktionen mit dem Modul $k = \sin\frac{\pi}{12}$, und für die biquadratischen Reste die elliptischen Funktionen mit dem Modul $k = \sin\frac{\pi}{4} = \sqrt{\frac{1}{2}}$, die Lemniskatenfunktionen, angewendet werden, also in allen diesen Fällen periodische Funktionen, welche für die besonderen den aliquoten Theilen ihrer Perioden entsprechenden Werthe ihrer Variabeln zu Wurzeln algebraischer Gleichungen mit ganzzahligen Coefficienten werden. Es war sehr natürlich, dafs Eisenstein

in dieser Anwendung der periodischen Funktionen die wahre Quelle auch für die Reciprocitätsgesetze höherer Potenzreste gefunden zu haben glaubte, so dafs er schon eine gröfsere Arbeit über dieselben ankündigte; es ist aber weder ihm selbst noch anderen bisher gelungen, mit Hülfe dieser Principien irgend welche höhere Reciprocitätsgesetze zu beweisen, oder auch nur aufzufinden. Seine eigenen Bemühungen in dieser Beziehung sind schon an den achten Potenzen gescheitert, für deren Reciprocitätsbeziehung er nur specielle Resultate hat gewinnen können. Ebenso hat Eisenstein in einer späteren Arbeit über die allgemeinen Reciprocitätsgesetze für die Reste der Potenzen, deren Exponent eine beliebige Primzahl ist, welche im Jahre 1850 durch Jacobi der Akademie mitgetheilt, und in den Monatsberichten derselben veröffentlicht ist, nur einen sehr beschränkten Fall ergründen können, nämlich denjenigen, in welchem eine der beiden zu vergleichenden Primzahlen eine nichtcomplexe ist. Er hat dazu auch nicht die Prinzipien gebraucht, auf welche er früher seine Hoffnung gesetzt hatte, sondern nur die Mittel der Kreistheilung angewendet, und zwar die von mir gefundenen Ausdrücke, welche die complexen Zahlen der Kreistheilung, in ihre wirklichen oder idealen Primfaktoren zerlegt, darstellen. Endlich ist noch eine Arbeit von Eisenstein zu erwähnen, in Crelle's Journal, Bd. 39, pg. 351, in welcher er darauf ausgeht, die allgemeinen Reciprocitätsgesetze durch Induktion zu finden. Der Weg, den er dabei einschlägt, hat aber nicht zum Ziele geführt und überhaupt kein Resultat ergeben.

Der wahre Grund, warum alle die hier genannten sehr verschiedenen, scharfsinnigen und für die quadratischen, kubischen und biquadratischen Reste auch durchaus sachgemäfsen Methoden auf die Erforschung der höheren Reciprocitätsgesetze entweder gar keine, oder doch nur eine sehr beschränkte Anwendung gestattet haben, liegt in einem eigenthümlichen Umstande, welcher für die, diesen Gesetzen zu Grunde zu legenden complexen Zahlen eintritt, sobald man über die vierten Potenzen hinausgeht, nämlich in der unendlichen Anzahl der Einheiten. Die complexen Primzahlen haben in Beziehung darauf, ob sie Reste oder Nichtreste sind, ganz andere Charaktere, je nachdem man die Einheiten, mit welchen sie behaftet sein können, anders und anders wählt; die einfachsten Reciprocitätsgesetze lassen sich darum erst dann aufstellen, wenn man diese Einheiten den richtigen Bestimmungen unterworfen hat, d. h. wenn man die complexen Primzahlen

um die es sich handelt, in derjenigen Form gewählt hat, welche für die vorliegende Frage die angemessenste ist. Da ferner die Reciprocitätsgesetze für die λten Potenzreste, wo λ als Primzahl angenommen wird, zwischen je zwei aus λten Wurzeln der Einheit gebildeten complexen Primzahlen aufgestellt werden müssen, so gehört zur Erforschung dieser Gesetze nothwendig eine vollständige Theorie dieser complexen Zahlen, namentlich ihrer Primfaktoren und Einheiten. Es gehört dazu auch wesentlich die von mir in die Zahlentheorie eingeführte Erweiterung des Gaufsischen Prinzips durch die idealen Zahlen, ohne welche die complexen Zahlen in den meisten Fällen gar keine wahren Primfaktoren haben würden, nämlich keine solchen, welche in einer gegebenen complexen Zahl als die unveränderlichen Elemente derselben enthalten sein müfsten. Es gehört selbst die Kenntnifs der Klassenanzahl dieser idealen Zahlen dazu, und die Unterscheidung derjenigen Exponenten λ, für welche diese Klassenanzahl durch λ nicht theilbar ist, von denjenigen, welchen eine durch λ theilbare Klassenanzahl zukommt, so wie auch die Kenntnifs der besonderen Eigenschaften, welche die Einheiten besitzen, je nachdem der Wurzelexponent λ der einen oder der anderen Art angehört. Erst nachdem ich diese ganze Theorie der aus λten Wurzeln der Einheit gebildeten complexen Zahlen, und zwar mit der schon in meiner ersten Schrift über diesen Gegenstand ausgesprochenen Absicht, sie für die höheren Reciprocitätsgesetze benutzen zu können, in hinreichender Vollständigkeit erarbeitet hatte, ging ich an die Erforschung dieser Gesetze selbst, und es gelang mir im Jahre 1847 dieselben für die Reste der λten Potenzen, wenn λ eine Primzahl ist, für welche die Klassenanzahl der idealen Zahlen durch λ nicht theilbar ist, in ihrer einfachsten Form aufzufinden. Nachdem ich dieselben durch berechnete Tafeln in ziemlich grofser Ausdehnung verificirt hatte, theilte ich sie im Januar 1848 an Hrn. Dirichlet und Jacobi und später, im Mai 1850, auch der Königl. Akademie mit, m. s. die Monatsberichte. Es blieb nun noch übrig, die gefundenen Gesetze zu beweisen. Das Mittel, zu welchem ich in dieser Absicht zuerst griff, war die Theorie der Kreistheilung, welche bereits die einfachsten Beweise aller bisher ergründeten Reciprocitätsgesetze geliefert hatte, und von welcher ich um so mehr erwarten konnte, da sie durch meine Arbeiten über complexe Zahlen wesentlich gefördert worden war. Ich fand auch in der That durch dieses Mittel die einfachen Beweise der

Ergänzungssätze zu dem allgemeinen Reciprocitätsgesetze, nämlich die Charaktere oder die Indices der Einheiten und der Zahl $1-\alpha$, des Primfaktors von λ, welche Beweise ich gleichzeitig mit dem, nur durch Induktion erhärteten, allgemeinen Reciprocitätsgesetze der Königl. Akademie mitgetheilt habe. Ich erkannte aber bald, daſs die Kreistheilung allein die vollständigen Reciprocitätsgesetze für λte Potenzreste zwischen je zwei complexen Primzahlen nicht geben könne, wenn λ gröſser als drei ist, oder was dasselbe ist, wenn auſser den einfachen Einheiten ± 1, $\pm \alpha$, ... $\pm \alpha^{\lambda-1}$ unendlich viele Einheiten existiren. Der Grund ist der, daſs in allen complexen Zahlen der Kreistheilung die conjugirten, wirklichen oder idealen Primfaktoren nur in solchen Verbindungen vorkommen, daſs, wenn man einen derselben mit einer Einheit $E(\alpha)$, für welche $E(\alpha) = E(\alpha^{-1})$ ist, und die ihm conjugirten Primfaktoren mit den entsprechenden conjugirten Einheiten multiplicirt, diese complexen Zahlen der Kreistheilung ganz ungeändert bleiben. Wegen dieses Umstandes kann die Kreistheilung keine Reciprocitätsgesetze geben, bei denen die verschiedene Wahl solcher Einheiten in den complexen Primzahlen einen Unterschied des Potenzcharakters bewirkt. Dieses der Theorie der Kreistheilung unübersteigliche Hinderniſs für die Erkenntniſs der allgemeinen Reciprocitätsgesetze ist auch durch andere Methoden in Jacobi's und Eisenstein's Arbeiten selbst nicht in irgend einem besonderen Falle besiegt worden. Den ersten Schritt über diese Gränze hinaus habe ich in einem Beweise des Reciprocitätsgesetzes für λte Potenzreste, welches unter je zwei conjugirten complexen Primzahlen Statt hat, in Crelle's Journal, Bd. 50, pag. 212, gemacht, und zwar mit Hülfe gewisser, aus Einheiten gebildeter Ausdrücke, welche die Lagrangesche Resolvente der Kreistheilung als speciellen Fall in sich enthalten, und darum als eine Verallgemeinerung der Kreistheilung angesehen werden können. Aber auch dieses neue, für die Theorie der complexen Zahlen überhaupt sehr nützliche Instrument, welches in der gegenwärtigen Untersuchung ebenfalls vielfache Anwendung finden wird, hat mir die vollständigen Beweise der Reciprocitätsgesetze nicht gegeben, und ich habe mich endlich genöthigt gesehen, den bis dahin eingeschlagenen Weg der Verallgemeinerung der Kreistheilung aufzugeben und andere Mittel und Wege aufzusuchen. Ich wendete meine Aufmerksamkeit auf die Methode des zweiten Gauſsischen Beweises des *theorema fundamentale,* welcher auf der Theorie der quadratischen Formen beruht. Dieser Beweis, obgleich seine Methode bis dahin

auf die quadratischen Reste beschränkt geblieben war, schien mir in seinen Prinzipien denjenigen Charakter der Allgemeinheit zu haben, welcher hoffen liefs, dafs dieselben mit Erfolg auch auf die Untersuchung der Reste höherer Potenzen möchten angewendet werden können, und diese meine Erwartung ist in der That erfüllt worden.

Der Hauptnerv dieses zweiten Gaufsischen Beweises liegt in der Eintheilung der Klassen der quadratischen Formen einer gegebenen Determinante in *Genera,* welche durch die Charaktere der Klassen bestimmt sind, und namentlich darin, dafs die Anzahl der wirklich vorhandenen *Genera* nur höchstens halb so grofs ist, als die Anzahl der angebbaren, d. h. derjenigen, welche vermöge der vorhandenen Charaktere der Klassen möglicherweise Statt haben könnten. Nachdem dieser Punkt bei Gaufs durch die Untersuchung der *Classes ancipites* festgestellt ist, wird der Beweis des Reciprocitätsgesetzes in der Art geführt, dafs gezeigt wird: wenn dasselbe nicht Statt hätte, so müfste die Anzahl der wirklich vorhandenen *Genera* gröfser sein, als die Hälfte der blofs angebbaren. Um nun nach diesen Prinzipien die Reciprocitätsgesetze der Reste und Nichtreste der λten Potenzen zu ergründen, hat man anstatt der Formen des zweiten Grades mit zwei Unbestimmten hier Formen des λten Grades mit λ Unbestimmten zu Grunde zu legen, und zwar Formen, deren Coefficienten nicht gewöhnliche ganze Zahlen, sondern aus λten Wurzeln der Einheit gebildete complexe ganze Zahlen sind. Die Theorie dieser Formen des λten Grades mufs auch bis zu dem Punkte ergründet werden, der in der Theorie der quadratischen Formen der Stelle entspricht, an welcher der Gaufsische Beweis seinen Platz gefunden hat, und sogar noch bedeutend weiter, weil der Umstand, dafs in der Theorie der λten Potenzreste nicht nur Reste von Nichtresten, sondern auch die Nichtreste von $\lambda - 1$ verschiedenen Arten zu unterscheiden sind, nöthig macht, dafs wenigstens in gewissen Hauptfällen die Anzahl der wirklich vorhandenen *Genera* genau ermittelt, und nicht blofs eine Gränze gefunden werde, welche diese Anzahl niemals überschreiten kann. Diese schwer zu bewältigende Arbeit hat offenbar der Anwendung der Principien dieses Gaufsischen Beweises auf die Untersuchung der höheren Potenzreste bisher entgegengestanden. Ich selbst würde auch nicht gewagt haben, diese Arbeit zu unternehmen, wenn ich nicht die Überzeugung gehabt hätte, dafs gewifse, für den vorliegenden Zweck passend zu wählende specielle Formen des λten

Grades mit complexen Coefficienten ausreichen möchten, und wenn ich nicht in meinem Principe der idealen Faktoren der complexen Zahlen ein Mittel gehabt hätte, die Betrachtung der zerlegbaren Formen des λten Grades durch die bei weitem einfachere Betrachtung der complexen Zahlen, welche aus den Wurzeln einer Gleichung des Grades λ gebildet sind, und der idealen Faktoren derselben, zu ersetzen.

Ich gebrauche zu dem vorliegenden Zwecke zwei über einander liegende Theorieen complexer Zahlen, deren niedere, nur die Wurzeln der Gleichung $\alpha^\lambda = 1$ enthaltende, aus meinen früheren Arbeiten als bekannt gelten kann, und deren höhere aufser dieser λten Wurzel der Einheit noch die Wurzel einer Gleichung des λten Grades enthält. Diese höhere Theorie der complexen Zahlen wird alsdann weiter in drei verschiedene Stufen getheilt, welche zu einander in derselben Beziehung stehen, wie die *Ordines derivati* zu dem *Ordo primitivus,* welches Verhältnifs in der Theorie der complexen Zahlen die eigenthümliche Bedeutung hat, dafs gewisse complexe Zahlen, welche in der niederen Stufe als wirkliche ganze Zahlen nicht darstellbar sind, sondern nur als wirkliche gebrochene, und welche darum als ideale gelten müssen, innerhalb der höheren Stufe als wirkliche und ganze complexe Zahlen dargestellt werden können. Der Gedanke, welcher dieser Anwendung verschiedener einander übergeordneter Theorieen der complexen Zahlen zu Grunde liegt, nämlich dafs dasjenige, was in der Theorie der gewöhnlichen Zahlen schwer oder vielleicht gar nicht zu finden ist, in einer richtig gewählten complexen Theorie gesucht werden mufs, und dafs ferner dasjenige, was auch diese versagt, weiter in einer passenden höheren Theorie zu suchen ist und so fort, bis das vorgesteckte Ziel vollständig erreicht ist, darf übrigens nur als eine einfache Consequenz des ursprünglichen Gaufsischen Gedankens der Einführung complexer ganzer Zahlen überhaupt angesehen werden. Man hat auch bereits Beispiele des Aufsteigens von einer complexen Theorie zu einer höheren, denn wenn z. B. bei dem Jacobischen Beweise des kubischen Reciprocitätsgesetzes $\alpha^3 = 1$ und $x^p = 1$ ist, und p Primzahl der Form $6n+1$, so ist die Anwendung der Lagrangeschen Resolvente der Kreistheilung, welche die beiden Wurzeln α und x zugleich enthält, nichts anderes, als das Aufsteigen von complexen Zahlen, welche α allein enthalten, zu complexen Zahlen der höheren, die Wurzeln α und x enthaltenden Theorie.

Nachdem ich nun den gegenwärtigen Standpunkt der Wissenschaft in der Theorie der Potenzreste, so wie auch die leitenden Gedanken für den in derselben zu machenden weiteren Fortschritt angegeben habe, werde ich in der gegenwärtigen Abhandlung die Theorie derjenigen complexen Zahlen, auf welche der hier zu gebende Beweis der allgemeinen Reciprocitätsgesetze sich gründet, in soweit entwickeln, als es für den vorliegenden Zweck nöthig ist, und sodann den Beweis der Reciprocitätsgesetze selbst folgen lassen, durch welchen dieselben genau in derjenigen Ausdehnung, in welcher ich sie im Mai 1850 der Königlichen Akademie ohne Beweise mitgetheilt habe, vollständig nnd streng begründet werden.

§. 1.

Definition und allgemeine Eigenschaften der complexen Zahlen, welche der gegenwärtigen Untersuchung zu Grunde gelegt werden.

Die in der folgenden Untersuchung in Anwendung kommenden complexen Zahlen sollen aufser den Wurzeln der Gleichung des $\lambda-1$ ten Grades

$$(1.) \qquad \alpha^{\lambda-1}+\alpha^{\lambda-2}+\alpha^{\lambda-3}+\ldots+\alpha+1=0$$

auch die Wurzeln der Gleichung des λten Grades

$$(2.) \qquad w^{\lambda}=D(\alpha)$$

enthalten, in welcher $D(\alpha)$ eine nur die Wurzel α enthaltende ganze complexe Zahl ist. Wenn diese Zahl $D(\alpha)$, welche als Determinante der, die Wurzeln α und w enthaltenden, complexen Zahlen bezeichnet werden soll, nicht eine vollständige λte Potenz ist, so ist diese Gleichung (2.) eine irreductible, in dem Sinne, dafs sie nicht in Faktoren zerlegt werden kann, deren Coefficienten ganze nur die Wurzel α enthaltende complexe Zahlen sind.

Jede ganze rationale Funktion der Wurzeln α und w mit ganzzahligen Coefficienten soll als eine aus diesen Wurzeln gebildete ganze complexe Zahl angesehen, und kurz als complexe Zahl in w bezeichnet werden. Weil vermöge der Gleichung (2.) die Potenzen von w, welche höher sind, als die $\lambda-1$te, durch niedere ersetzt werden können, so folgt, dafs jede complexe Zahl in w in die Form

$$(3.) \qquad F(w)=A+A_1 w+A_2 w^2+\ldots+A_{\lambda-1} w^{\lambda-1}$$

gesetzt werden kann, in welcher die Coefficienten $A, A_1, A_2, \ldots A_{\lambda-1}$ nur

die Wurzel α enthaltende complexe ganze Zahlen sind, welche zum Unterschiede von den aufserdem auch w enthaltenden kurz als **complexe Zahlen in α** bezeichnet werden. Aus der Irreductibilität der Gleichung (2.) folgt auch, dafs eine jede gegebene complexe Zahl in w nur auf eine einzige Weise in diese Form gesetzt werden kann.

Die zu einer complexen Zahl $F(w)$ **conjugirten** Zahlen sind diejenigen, welche man erhält, indem man der Wurzel w ihre λ verschiedenen Werthe $w, w\alpha, w\alpha^2, \ldots w\alpha^{\lambda-1}$ giebt. Das Produkt dieser λ conjugirten Zahlen

$$F(w)\, F(w\alpha)\, F(w\alpha^2) \ldots F(w\alpha^{\lambda-1}) = NF(w)$$

wird die Norm einer derselben genannt, und ist eine complexe Zahl in α.

Es soll ferner eine bestimmte Art dieser aus den Wurzeln der Gleichung (2.) gebildeten complexen Zahlen besonders betrachtet werden, in welcher diese Wurzeln nicht einzeln, sondern nur in folgenden bestimmten Verbindungen vorkommen:

$$(4.)\quad \begin{aligned} z_0 &= \varrho\,(1 + w + w^2 + \ldots + w^{\lambda-1}) \\ z_1 &= \varrho\,(1 + \alpha w + \alpha^2 w^2 + \ldots + \alpha^{\lambda-1} w^{\lambda-1}) \\ z_2 &= \varrho\,(1 + \alpha^2 w + \alpha^4 w^2 + \ldots + \alpha^{2\lambda-2} w^{\lambda-1}) \\ &\vdots \\ z_{\lambda-1} &= \varrho\,(1 + \alpha^{\lambda-1} w + \alpha^{2\lambda-2} w^2 + \ldots + \alpha^{(\lambda-1)^2} w^{\lambda-1}), \end{aligned}$$

wo ϱ als abgekürztes Zeichen für die sehr häufig vorkommende Zahl $1-\alpha$ gesetzt ist, welche Bedeutung dieser Buchstabe auch in dem Folgenden überall behalten soll.

Der allgemeine Ausdruck

$$z_k = \varrho\,(1 + \alpha^k w + \alpha^{2k} w^2 + \ldots + \alpha^{(\lambda-1)k} w^{\lambda-1})$$

kann auch in folgende Form gesetzt werden:

$$z_k = \frac{\rho\,(1 - D(\alpha))}{1 - \alpha_k w}$$

und giebt so

$$\alpha^k w = 1 - \frac{\rho\,(1 - D(\alpha))}{z_k} .$$

Multiplicirt man mit z_k und erhebt beide Seiten dieser Gleichung zur λten Potenz, so erhält man folgende Gleichung des λten Grades:

$$D(\alpha)\, z_k^\lambda = \Big(z_k - \varrho\,(1 - D(\alpha))\Big)^\lambda,$$

welcher, weil k in den Coefficienten nicht vorkommt, alle λ Werthe z_0, z_1,

$z_2, \ldots z_{\lambda-1}$ als Wurzeln genügen müssen. Schreibt man also z statt z_k und entwickelt nach Potenzen von z, so erhält man

$$(5.) \quad z^{\lambda} - \lambda\varrho z^{\lambda-1} + \frac{\lambda(\lambda-1)}{1.2}\varrho^2(1-D(\alpha))z^{\lambda-2} - \ldots - \varrho^{\lambda}(1-D(\alpha))^{\lambda-1} = 0$$

welche Gleichung als die, der besonderen Art von complexen Zahlen in w zu Grunde liegende Gleichung anzusehen ist, in der Art, daſs eine jede rationale und ganze Funktion der Wurzeln derselben, welche ganze complexe Zahlen in α zu Coefficienten hat, als eine complexe Zahl dieser besonderen Art angesehen werden soll. Zur Unterscheidung von den allgemeineren complexen Zahlen in w sollen die aus den Wurzeln der Gleichung (5.) gebildeten, als complexe Zahlen in z bezeichnet werden.

Nimmt man zwei verschiedene Wurzeln der Gleichung (5.):

$$z_k = \frac{\varrho(1-D(\alpha))}{1-\alpha^k w}, \quad z_h = \frac{\varrho(1-D(\alpha))}{1-\alpha^h w},$$

und eliminirt die Gröſse w aus diesen Ausdrücken, so erhält man

$$(6.) \qquad z_k z_h = \frac{\varrho(1-D(\alpha))}{\alpha^h - \alpha^k}(\alpha^h z_h - \alpha^k z_k).$$

Diese Formel zeigt, wie das Produkt zweier beliebigen, aber verschiedenen Wurzeln der Gleichung (5.) als lineäre Funktion derselben Wurzeln ausgedrückt wird, und zwar mit Coefficienten welche ganze complexe Zahlen in α sind, weil der Nenner $\alpha^h - \alpha^k$ gegen den Faktor $\varrho = 1 - \alpha$ des Zählers hinweggehoben werden kann. Es läſst sich aber auch das Quadrat einer jeden Wurzel z_k als lineäre Funktion aller Wurzeln darstellen; denn man hat aus der Gleichung (5.) die Summe aller Wurzeln

$$(7.) \qquad z_0 + z_1 + z_2 + \ldots + z_{\lambda-1} = \lambda\varrho,$$

also wenn man mit z_k multiplicirt und die Produkte zweier verschiedenen Wurzeln lineär ausdrückt, so erhält man z_k^2 als lineäre Funkion aller Wurzeln und zwar ebenfalls mit ganzen complexen Coefficienten. Da also das Produkt je zweier Wurzeln der Gleichung (5.), sie mögen verschieden oder auch dieselben sein, als ganze lineäre Funktion aller Wurzeln mit ganzen Coefficienten sich darstellen läſst, so folgt unmittelbar, daſs dasselbe auch für ein jedes Produkt beliebig vieler Wurzeln der Fall ist, und darum auch für jede ganze rationale Funktion der Wurzeln. Man hat daher folgenden Satz:

(I.) Jede ganze rationale Funktion der Wurzeln $z_0, z_1, \ldots z_{\lambda-1}$ läſst sich als lineäre Funktion dieser Wurzeln darstellen, und

wenn die Coefficienten dieser ganzen rationalen Funktion ganze complexe Zahlen in α sind, so sind auch die Coefficienten ihres Ausdrucks in der lineären Form nur ganze complexe Zahlen in α.

Die complexen Zahlen in z lassen sich also stets in folgender Form darstellen:

(8.) $$F(z) = C + Bz + B_1 z_1 + B_2 z_2 + \dots + B_{\lambda-1} z_{\lambda-1},$$

in welcher die Coefficienten C, B, B_1, ... $B_{\lambda-1}$ ganze complexe Zahlen in α sind. Man kann auch diese aus $\lambda + 1$ Gliedern bestehende Form mit Hülfe der Gleichung (7.) so vereinfachen, dafs sie ein Glied weniger enthält. Das erste Glied C läfst sich auf diese Weise im Allgemeinen nicht entfernen, ohne dafs die Coefficienten dieser Form Brüche mit dem Nenner $\lambda\varrho$ werden, jedes andere Glied aber kann weggeschafft werden, ohne dafs dieser Übelstand eintritt. Schafft man das letzte Glied weg, so erhält man die Form

(9.) $$F(z) = C + Bz + B_1 z_1 + B_2 z_2 + \dots + B_{\lambda-2} z_{\lambda-2}.$$

Diese Form ist eine solche, in welche eine gegebene complexe Zahl $F(z)$ sich nur auf *eine* Weise setzen läfst. Wenn nämlich die Zahl $F(z)$ zwei verschiedene Darstellungen derselben Form hätte, so würde durch Subtraktion derselben eine Gleichung von der Form

(10.) $$0 = c + bz + b_1 z_1 + b_2 z_2 + \dots + b_{\lambda-2} z_{\lambda-2}$$

entstehen, deren Coefficienten c, b, b_1, ... $b_{\lambda-2}$ nicht alle zugleich gleich Null wären. Drückt man nun vermittelst der Ausdrücke (4.) die Wurzeln z, z_1, ... $z_{\lambda-2}$ alle durch w aus, so erhält man eine Gleichung von folgender Form:

(11.) $$o = c + \varrho m + \varrho m_1 w + \varrho m_2 w^2 + \dots + \varrho m_{\lambda-1} w^{\lambda-1},$$

in welcher die Gröfsen m, m_1, m_2, ... $m_{\lambda-1}$ folgende Werthe haben:

$$\begin{aligned}
m &= b + b_1 + b_2 + \dots + b_{\lambda-2}\\
m_1 &= b + \alpha b_1 + \alpha^2 b_2 + \dots + \alpha^{\lambda-2} b_{\lambda-2}\\
m_2 &= b + \alpha^2 b_1 + \alpha^4 b_2 + \dots + \alpha^{2\lambda-4} b_{\lambda-2}\\
&\vdots\\
m_{\lambda-1} &= b + \alpha^{\lambda-1} b_1 + \alpha^{2\lambda-2} b_2 + \dots + \alpha^{(\lambda-1)(\lambda-2)} b_{\lambda-2}
\end{aligned}$$

Wegen der Irreductibilität der Gleichung $w^\lambda = D(\alpha)$ kann aber die Gleichung (11.) nicht anders bestehen, als wenn die Coefficienten der einzelnen Potenzen von w alle gleich Null sind, man hat daher

$$m_1 = 0,\ m_2 = 0,\ \ldots.\ m_{\lambda-1} = 0 \text{ und } c + \varrho m = 0.$$

Die ersten $\lambda - 1$ Gleichungen geben nothwendig

$$b = 0,\ b_1 = 0,\ b_2 = 0,\ \ldots.\ b_{\lambda-2} = 0,$$

weil die Determinante dieses Systems lineärer Gleichungen nicht gleich Null ist, hieraus folgt sodann, dafs auch $m = 0$ sein mufs, und darum auch $c = 0$. Die Gleichung (10.) kann also nicht bestehen, ohne dafs alle ihre Coefficienten einzeln gleich Null sind, woraus folgt, dafs die complexe Zahl $F(z)$ nur auf eine einzige Weise in die Form (9.) gesetzt werden kann.

Als die conjugirten complexen Zahlen zu $F(z)$ sollen diejenigen betrachtet werden, welche man aus dieser erhält, indem man die Indices aller Wurzeln $z, z_1, z_2, \ldots. z_{\lambda-2}$ um eine und dieselbe Zahl vermehrt, wobei, wenn diese Indices gröfser als $\lambda - 1$ werden, statt derselben nur ihre kleinsten Reste nach dem Modul λ zu nehmen sind. Die λ conjugirten Zahlen, welche man auf diese Weise erhält, sollen kurz durch $F(z)$, $F(z_1)$, $F(z_2)$, ... $F(z_{\lambda-1})$ bezeichnet werden, so dafs allgemein

$$F(z_k) = C + Bz_k + B_1 z_{k+1} + B_2 z_{k+2} + \ldots. + B_{\lambda-1} z_{k+\lambda-1}$$

eine jede conjugirte Zahl zu $F(z)$ darstellt. Das Produkt aller conjugirten Zahlen

$$F(z)\ F(z_1)\ F(z_2)\ \ldots\ldots\ F(z_{\lambda-1}) = NF(z),$$

welches die Norm einer derselben ausmacht, ist als symmetrische Funktion aller Wurzeln der Gleichung (2.) nur eine complexe Zahl in α.

§. 2.

Gegenseitiges Verhältnifs der complexen Zahlen in z und in w.

Alle ganzen complexen Zahlen in z sind zugleich auch ganze complexe Zahlen in w, denn die Wurzeln $z_0, z_1, z_2 \ldots. z_{\lambda-1}$ selbst sind ganze rationale Funktionen von w mit ganzen Coefficienten. Es läfst sich auch umgekehrt jede ganze rationale Funktion von w als lineäre Funktion der Wurzeln $z_0, z_1, z_2 \ldots. z_{\lambda-1}$ darstellen, jedoch im Allgemeinen nur so, dafs in den Coefficienten dieser lineären Funktion Brüche vorkommen. Durch Umkehrung des Systems der Gleichungen, welche $z_0, z_1 \ldots. z_{\lambda-1}$ als Funktionen von w geben, erhält man nämlich

$$(1.)\quad \begin{aligned}
\lambda\varrho &= z_0 + z_1 + z_2 + \dots + z_{\lambda-1}\\
\lambda\varrho w &= z_0 + \alpha^{-1} z_1 + \alpha^{-2} z_2 + \dots + \alpha^{-\lambda+1} z_{\lambda-1}\\
\lambda\varrho w^2 &= z_0 + \alpha^{-2} z_1 + \alpha^{-4} z_2 + \dots + \alpha^{-2\lambda+2} z_{\lambda-1}\\
&\vdots\\
\lambda\varrho w^{\lambda-1} &= z_0 + \alpha^{-(\lambda-1)} z_1 + \alpha^{-(2\lambda-2)} z_2 + \dots + \alpha^{-(\lambda-1)(\lambda-1)} z_{\lambda-1}
\end{aligned}$$

Multiplicirt man nun den allgemeinen Ausdruck einer ganzen complexen Zahl in w

$$F(w) = A + A_1 w + A_2 w^2 + \dots + A_{\lambda-1} w^{\lambda-1}$$

mit $\lambda\varrho$, und drückt die Gröſsen $\lambda\varrho$, $\lambda\varrho w$, $\lambda\varrho w^2$ .... $\lambda\varrho w^{\lambda-1}$ nach diesen Formeln durch die Wurzeln z_0, z_1 .... $z_{\lambda-1}$ aus, so erhält man einen Ausdruck des $\lambda\varrho F(w)$ als lineäre Funktion dieser Wurzeln mit ganzen Coefficienten, welcher durch Anwendung der Summenzeichen sich folgendermaaſsen darstellen läſst:

$$\lambda\varrho F(w) = \sum_0^{\lambda-1}{}_k \sum_0^{\lambda-1}{}_h A_k \alpha^{-kh} z_h.$$

Wenn nun mittelst der ersten der Gleichungen (1.) $z_{\lambda-1}$ weggeschafft und durch ϱ dividirt wird, so wird:

$$(2.)\qquad \lambda F(w) = \sum_0^{\lambda-1}{}_k \sum_0^{\lambda-2}{}_h \frac{A_k(\alpha^{-kh} - \alpha^k)}{1-\alpha} z_h + \lambda \sum_0^{\lambda-1}{}_k A_k.$$

Da der Nenner $1-\alpha$ gegen den Faktor $\alpha^{-kh} - \alpha^k$ des Zählers sich wegheben lässt, so sind alle Coefficienten dieses lineären Ausdrucks ganz, und man hat demnach den Satz:

(I.) Das λfache einer jeden ganzen complexen Zahl in w läſst sich stets als ganze complexe Zahl in z darstellen.

Für die speciellere complexe Zahl $(1-w)^n$, wo $n<\lambda$, hat man

$$A = 1,\ A_1 = -\frac{n}{1}\ A_2 = +\frac{n(n-1)}{2}, \dots\dots$$

und folglich

$$\lambda(1-w)^n = \sum_0^{\lambda-2}{}_h \frac{(1-\alpha^{-h})^n - (1-\alpha)^n}{1-\alpha} z_h.$$

Weil die Zahl λ den Faktor $\varrho = 1-\alpha$ genau $\lambda - 1$ mal enthält, und auſserdem nur Einheiten, so ist $\varrho^{\lambda-1} = \lambda E(\alpha)$, wo $E(\alpha)$ eine Einheit bezeichnet; multiplicirt man daher mit $E(\alpha)$, und dividirt durch ϱ^{n-1}, so erhält man:

$$\varrho^{\lambda-n}(1-w)^n = E(\alpha)\sum_{0}^{\lambda-2}{}_k \left(\left(\frac{1-\alpha^{-k}}{1-\alpha}\right)^n - 1\right) z_k\,.$$

Hieraus folgt, dafs $\varrho^{\lambda-n}(1-w)^n$ als ganze complexe Zahl in z sich darstellen läfst, wenn n eine ganze positive Zahl und kleiner als λ ist.

Die nothwendigen und hinreichenden Bedingungen dafür, dafs die allgemeine complexe Zahl $F(w)$ selbst, und nicht blofs das λfache derselben, als ganze complexe Zahl in z mit ganzen Coefficienten sich darstellen läfst, liegen vermöge der Gleichung (2.) darin, dafs die Congruenz

$$\sum_{0}^{\lambda-1}{}_k A_k\,(\alpha^{-hk} - \alpha^k) \equiv 0, \text{ mod. } \lambda\varrho,$$

für alle Werthe des $h = 0, 1, 2, \dots \lambda-2$ Statt habe, welche, wenn h in $h-1$ verwandelt und durch α^k dividirt wird, auch so dargestellt werden kann:

$$\text{(3.)}\qquad \sum_{1}^{\lambda-1}{}_k A_k\,(\alpha^{-hk} - 1) \equiv 0, \text{ mod. } \lambda\varrho,$$

für $h = 1, 2, 3 \dots \lambda-1$. Anstatt des Moduls $\lambda\varrho$ kann man, weil λ, abgesehen von einer Einheit, der $\lambda-1$ten Potenz von ϱ gleich ist, auch den Modul ϱ^λ wählen. Entwickelt man nun

$$\alpha^{-hk} = (1-(1-\alpha^{-h}))^k$$

nach dem binomischen Satze und setzt der Kürze wegen

$$\sum_{1}^{\lambda-1}{}_k \frac{k(k-1)\,\dots\dots\,(k-n+1)}{1.\,2\,\dots\dots\,n} A_k = G_k\,,$$

so geht die Congruenz (3.) in folgende über:

$$\text{(4.)}\qquad \begin{aligned} -G_1(1-\alpha^{-h}) + G_2(1-\alpha^{-h})^2 - G_3(1-\alpha^{-h})^3 + \dots \\ + G_{\lambda-1}(1-\alpha^{-h})^{\lambda-1} \equiv 0, \text{ mod. } \varrho^\lambda. \end{aligned}$$

Hebt man aus dieser Congruenz und ihrem Modul den gemeinschaftlichen Faktor $1-\alpha^{-h}$ hinweg, und giebt sodann dem h alle Werthe $h = 1, 2, 3, \dots\, \lambda-1$, welchen man auch den Werth $h = 0$ hinzufügen kann, weil für diesen die Congruenz identisch erfüllt ist, so erhält man durch Addition:

$$G_1 \equiv 0, \quad \text{mod. } \varrho^{\lambda-1}.$$

Läfst man nun das erste Glied aus der Congruenz (4.) hinweg, da dasselbe congruent Null ist nach dem Modul ϱ^λ, hebt sodann den gemeinschaftlichen

Faktor $(1-\alpha^{-h})^2$ aus dieser Congruenz und dem Modul heraus, und bildet die Summe für alle Werthe $h = 0, 1, 2, \ldots. \lambda - 1$, so erhält man

$$G_2 \equiv 0, \quad \text{mod. } \varrho^{\lambda-2}.$$

In derselben Weise weiter schliefsend erhält man allgemein

$$G_k \equiv 0, \quad \text{mod. } \varrho^{\lambda-k},$$

für $k = 1, 2, 3, \ldots. \lambda - 1$. Diese $\lambda - 1$ Congruenzen müssen also nothwendig erfüllt sein, damit $F(w)$ als ganze complexe Zahl in z sich darstellen lasse. Dafs die Erfüllung dieser Congruenzen auch zugleich die hinreichende Bedingung hierfür ist, wird leicht gezeigt, wenn man $F(w)$ nach Potenzen von $1 - w$ entwickelt, wodurch man

$$F(w) = G + G_1(1-w) + G_2(1-w)^2 + \ldots. + G_{\lambda-1}(1-w)^{\lambda-1}$$

erhält. Wenn nämlich $G_k \equiv 0$, mod. $\varrho^{\lambda-k}$ ist, so ist nach dem oben bewiesenen Satze: dafs $\varrho^{\lambda-k}(1-w)^k$ als ganze complexe Zahl in z sich darstellen läfst, nothwendig jeder einzelne Theil dieser Entwickelung von $F(w)$, und darum auch $F(w)$ selbst, als ganze complexe Zahl in z darstellbar. Das gefundene Resultat giebt folgenden Lehrsatz:

(II.) Die nothwendigen und hinreichenden Bedingungen dafür, dafs eine gegebene ganze complexe Zahl in w:

$$F(w) = A + A_1 w + A_2 w^2 + \ldots. + A_{\lambda-1} w^{\lambda-1}$$

als ganze complexe Zahl in z sich darstellen läfst, sind in folgenden $\lambda - 1$ Congruenzen enthalten:

$$\begin{array}{rl}
A_1 + 2A_2 + 3A_3 + 4A_4 + \ldots. \quad + (\lambda-1)A_{\lambda-1} & \equiv 0, \text{ mod. } \varrho^{\lambda-1}, \\
A_2 + 3A_3 + 6A_4 + \ldots. \quad + \frac{(\lambda-1)(\lambda-2)}{1.\,2.} A_{\lambda-1} & \equiv 0, \text{ mod. } \varrho^{\lambda-2}, \\
A_3 + 4A_4 + \ldots. + \frac{(\lambda-1)(\lambda-2)(\lambda-3)}{1.\,2.\,3} A_{\lambda-1} & \equiv 0, \text{ mod. } \varrho^{\lambda-3}, \\
\vdots \qquad & \\
A_{\lambda-1} & \equiv 0. \text{ mod. } \varrho.
\end{array}$$

§. 3.

Die den Gleichungswurzeln der complexen Zahlen in w entsprechenden Congruenzwurzeln.

Es sind nun zunächst die Bedingungen zu untersuchen, unter welchen eine gegebene complexe Primzahl in α, welche in dieser niederen Theorie

wirklich oder auch ideal sein kann, ein Divisor der Norm einer complexen Zahl der höheren Theorie in w ist. Diese Untersuchung wird zugleich auch für die Normen der complexen Zahlen in z ausreichen, weil jede ganze complexe Zahl in z als eine ganze complexe Zahl in w dargestellt werden kann.

Sei $\phi(\alpha)$ irgend eine wirkliche oder ideale complexe Primzahl in α, jedoch nicht eine von denen, welche in der Determinante $D(\alpha)$ enthalten sind und auch nicht die besondere Primzahl $\varrho = 1 - \alpha$. Dieselbe sei ein Primfaktor der nicht complexen Primzahl q, und es sei t der Exponent, zu welchem q gehört, nach dem Modul λ, so dafs $q^t \equiv 1$, mod. λ ist, und t der kleinste Exponent welcher dieser Bedingung entspricht, alsdann hat man, wie aus der Theorie der complexen Zahlen in α bekannt ist:

$$N\phi(\alpha) = \phi(\alpha)\,\phi(\alpha^2)\,\phi(\alpha^3)\,\ldots\ldots\,\phi(\alpha^{\lambda-1}) = q^t.$$

Ferner ist für jede nicht durch $\phi(\alpha)$ theilbare wirkliche complexe Zahl $D(\alpha)$

$$D(\alpha)^{\frac{1}{\lambda}(N\phi(\alpha)-1)} = D(\alpha)^{\frac{1}{\lambda}(q^t-1)} \equiv \alpha^i, \quad \text{mod. } \phi(\alpha),$$

wo i eine der Zahlen $0, 1, 2, \ldots\ldots \lambda - 1$ ist, und es ist $D(\alpha)$ ein λter Potenzrest von $\phi(\alpha)$, wenn $i = 0$ ist, ein Nichtrest, wenn i nicht gleich Null ist, und zwar ein Nichtrest der $i$ten Klasse. Es sei endlich

$$F(w) = A + A_1 w + A_2 w^2 + \ldots\ldots + A_{\lambda-1} w^{\lambda-1}$$

eine beliebige complexe Zahl in w.

Um nun zu untersuchen, ob $\phi(\alpha)$ ein Divisor von $NF(w)$ ist, wird $F(w)$ zur $q$ten Potenz erhoben, und zwar in der Art, dafs die den Faktor q enthaltenden Glieder dieser $q$ten Potenz weggelassen werden, wodurch man eine Congruenz nach dem Modul q erhält [1]. Weil in einem Polynom, welches zur $q$ten Potenz erhoben wird, wenn q Primzahl ist, aufser den $q$ten Potenzen der einzelnen Theile alle übrigen Glieder den Faktor q enthalten, so wird

$$(1.)\quad F(w)^q \equiv A^q + A_1^q w^q + A_2^q w^{2q} + \ldots\ldots + A_{\lambda-1}^q w^{(\lambda-1)q}, \text{ mod. } q.$$

[1] Die Congruenz zweier complexen Zahlen in w in Beziehung auf einen Modul, welcher eine nichtcomplexe Zahl, oder auch eine complexe Zahl in α ist, hat die Bedeutung, dafs wenn beide Seiten der Congruenz in die oben aufgestellte Normalform gesetzt werden, in welche eine gegebene complexe Zahl in w sich nur auf eine einzige Weise setzen läfst, die Coefficienten aller λ Glieder auf der einen Seite den entsprechenden auf der anderen Seite einzeln congruent sein müssen. Dasselbe gilt auch für die Congruenzen unter complexen Zahlen in z.

Erhebt man in derselben Weise t mal hinter einander zur $q$ten Potenz, so erhält man

(2.) $F(w)^{q^t} \equiv A^{q^t} + A_1^{q^t} w^{q^t} + A_2^{q^t} w^{2q^t} + \ldots + A_{\lambda-1}^{q^t} w^{(\lambda-1)q^t}$, mod. q.

Weil die Coefficienten A, A_1, A_2 .... $A_{\lambda-1}$ complexe Zahlen in α sind, und $q^t \equiv 1$, mod. λ, so hat man, wie aus der Theorie dieser complexen Zahlen bekannt ist:

$$A_h^{q^t} \equiv A_h \text{, mod. } q,$$

ferner ist

$$w^{q^t} = w w^{q^t-1} = w D(\alpha)^{\frac{1}{\lambda}(q^t-1)},$$

und weil

$$D(\alpha)^{\frac{1}{\lambda}(q^t-1)} \equiv \alpha^i \text{, mod. } \phi(\alpha),$$

so ist

$$w^{q^t} \equiv w\alpha^i \text{, mod. } \phi(\alpha).$$

Nimmt man nun in der Congruenz (2.) anstatt des Moduls q den Modul $\phi(\alpha)$, welcher ein Theiler von q ist, und setzt die gefundenen Ausdrücke für $A_h^{q^t}$ und w^{q^t} ein, so hat man

$$F(w)^{q^t} \equiv A + A_1 w\alpha^i + A_2 w^2 \alpha^{2i} + \ldots + A_{\lambda-1} w^{\lambda-1} \alpha^{(\lambda-1)i} \text{, mod. } \phi(\alpha),$$

welche Congruenz auch so dargestellt werden kann:

(3.) $$F(w)^{q^t} \equiv F(w\alpha^i) \text{, mod. } \phi(\alpha).$$

Erhebt man beide Seiten dieser Congruenz zu wiederholten Malen zur Potenz q^t, so erhält man daraus die verallgemeinerte

(4.) $$F(w)^{q^{ht}} \equiv F(w\alpha^{hi}) \text{, mod. } \phi(\alpha),$$

und wenn h gleich einem Vielfachen von λ genommen wird:

$$F(w)^{q^{k\lambda t}} \equiv F(w) \text{, mod. } \phi(\alpha),$$

aus welcher Congruenz unmittelbar folgender Satz hervorgeht:

(I.) Wenn irgend eine Potenz einer complexen Zahl $F(w)$ durch eine nicht in $\varrho D(\alpha)$ enthaltene, wirkliche oder ideale

Primzahl $\phi(\alpha)$ theilbar ist, so ist auch diese Zahl $F(w)$ selbst durch $\phi(\alpha)$ theilbar.

Es sollen nun in der Congruenz (4.) die beiden Fälle: erstens wo i nicht congruent Null ist, und zweitens wo i congruent Null ist, nach dem Modul λ, besonders betrachtet werden.

Wenn erstens i nicht $\equiv 0$, mod. λ, also die Determinante $D(\alpha)$ ein Nichtrest von $\phi(\alpha)$ ist, so gebe man dem h in der Congruenz (4.) nach einander die Werthe $0, 1, 2, \ldots. \lambda-1$, und multiplicire die so erhaltenen Congruenzen, so hat man:

$$(5.)\quad \begin{aligned} F(w)^{1+q^i+q^{2i}+\ldots+q^{(\lambda-1)i}} &\equiv F(w)F(w\alpha^i)F(w\alpha^{2i}) \\ &\ldots. F(w\alpha^{(\lambda-1)i}),\ \text{mod. } \phi(\alpha). \end{aligned}$$

Setzt man der Kürze wegen

$$1+q^i+q^{2i}+\ldots.+q^{(\lambda-1)i} = Q,$$

und bezeichnet das Produkt der λ conjugirten complexen Zahlen in w, als Norm, durch $NF(w)$, so ist

$$F(w)^Q \equiv NF(w),\ \text{mod. } \phi(\alpha).$$

Hieraus folgt nun, dafs die Norm von $F(w)$ niemals durch $\phi(\alpha)$ theilbar sein kann, ohne dafs eine Potenz von $F(w)$ durch $\phi(\alpha)$ theilbar ist, und weil gezeigt worden ist, dafs eine Potenz von $F(w)$ nicht durch $\phi(\alpha)$ theilbar sein kann, ohne dafs $F(w)$ selbst durch $\phi(\alpha)$ theilbar ist, so hat man folgenden Lehrsatz:

(II.) Wenn $\phi(\alpha)$ eine complexe Primzahl in α ist, in Beziehung auf welche die Determinante $D(\alpha)$ ein Nichtrest ist, so enthält die Norm einer complexen Zahl $F(w)$ nur dann den Faktor $\phi(\alpha)$, wenn $F(w)$ selbst durch $\phi(\alpha)$ theilbar ist.

Hieraus folgt ferner, dafs, wenn die Norm $NF(w)$ einen Primfaktor $\phi(\alpha)$ enthält, für welchen die Determinante $D(\alpha)$ Nichtrest ist, diese Norm den Primfaktor $\phi(\alpha)$ nothwendig λ mal, oder $k\lambda$ mal enthalten mufs.

Es sei nun zweitens $i\equiv 0$, mod. λ, also $\phi(\alpha)$ eine solche Primzahl, in Beziehung auf welche die Determinante $D(\alpha)$ ein λter Potenzrest ist, so hat man:

$$(6.) \qquad D(\alpha) \equiv \xi^{\lambda}, \quad \text{mod. } \phi(\alpha),$$

wo ξ eine wirkliche complexe Zahl in α ist. Die λ Wurzeln dieser Congruenz des λten Grades sind, wenn eine derselben durch ξ bezeichnet wird:

$$\xi, \ \xi\alpha, \ \xi\alpha^2, \ \ldots . \ \xi\alpha^{\lambda-1}.$$

Diese Congruenzwurzeln entsprechen vollständig den Wurzeln

$$w, \ w\alpha, \ w\alpha^2, \ \ldots . \ w\alpha^{\lambda-1}$$

der Gleichung

$$D(\alpha) = w^{\lambda},$$

und können denselben auf λ verschiedene Weisen zugeordnet werden, in der Art, dafs, wenn der bestimmten Gleichungswurzel w die Congruenzwurzel $\xi\alpha^{t}$ als die entsprechende zugeordnet wird, allgemein der Gleichungswurzel $w\alpha^{h}$ die Congruenzwurzel $\xi\alpha^{t+h}$ entspricht.

Hat man irgend eine ganze und rationale Gleichung unter ganzen complexen Zahlen in w, welche, wenn alle Glieder auf eine Seite gebracht werden, immer die Form

$$\Phi(w) = 0$$

annimmt, wo $\Phi(w)$ irgendwie aus Summen, Differenzen, Produkten oder Potenzen complexer Zahlen in w zusammengesetzt sein kann, so mufs $\Phi(w)$, wenn w als eine unbestimmte Gröfse aufgefafst wird, nothwendig den Faktor $w^{\lambda} - D(\alpha)$ enthalten, weil die Gleichung $w^{\lambda} - D(\alpha) = 0$ eine irreductible ist. Setzt man nun für w irgend eine der Congruenzwurzeln $\xi, \xi\alpha, \ldots \xi\alpha^{\lambda-1}$, so wird der Faktor $w^{\lambda} - D(\alpha)$, und mit ihm $\Phi(w)$ selbst, congruent Null nach dem Modul $\phi(\alpha)$. Man hat also folgenden Satz:

(III.) Aus einer jeden rationalen ganzen Gleichung unter complexen Zahlen in w erhält man eine richtige Congruenz nach einem Modul $\phi(\alpha)$, für welchen die Determinante λter Potenzrest ist, wenn man die Wurzel w durch irgend eine Wurzel der Congruenz

$$\xi^{\lambda} \equiv D(\alpha), \quad \text{mod. } \phi(\alpha),$$

ersetzt.

Wendet man diesen Satz auf die Norm einer complexen Zahl (Fw) an, so hat man aus der Gleichung

$$NF(w) = F(w)\,F(w\alpha)\,F(w\alpha^2)\,\ldots\ldots\,F(w\alpha^{\lambda-1})$$

die Congruenz:

(7.) $$NF(w) \equiv F(\xi)\,F(\xi\alpha)\,F(\xi\alpha^2)\,\ldots\ldots\,F(\xi\alpha^{\lambda-1}),\ \text{mod. } \phi(\alpha),$$

und durch diese folgenden Satz:

(IV.) Wenn die Norm einer complexen Zahl $F(w)$ durch die complexe Primzahl $\phi(\alpha)$ theilbar ist, für welche $D(\alpha)$ ein λter Potenzrest ist, so ist nothwendig eine der nur α enthaltenden complexen Zahlen $F(\xi\alpha^k)$, welche man erhält, indem man für w eine der entsprechenden Congruenzwurzeln setzt, durch $\phi(\alpha)$ theilbar;

und umgekehrt:

Wenn eine complexe Zahl $F(w)$ die Eigenschaft hat, dafs, wenn man für w eine der entsprechenden Congruenzwurzeln setzt, die daraus entstehende complexe Zahl in α durch $\phi(\alpha)$ theilbar ist, so ist $NF(w)$ theilbar durch $\phi(\alpha)$.

Setzt man in dem Ausdrucke einer beliebigen complexen Zahl in w

$$F(w) = A + A_1 w + A_2 w^2 + \ldots . + A_{\lambda-1} w^{\lambda-1},$$

für w nach einander die λ Werthe w, $w\alpha$, $w\alpha^2$, ... $w\alpha^{\lambda-1}$, multiplicirt die so erhaltenen Gleichungen der Reihe nach mit 1, α, α^{-h}, α^{-2h}, ... $\alpha^{-(\lambda-1)h}$ und addirt, so erhält man:

$$F(w) + \alpha^{-h} F(w\alpha) + \alpha^{-2h} F(w\alpha^2) + \ldots + \alpha^{-(\lambda-1)h} F(w\alpha^{\lambda-1}) = \lambda A_h w^h,$$

und wenn man anstatt w in dieser Gleichung die Congruenzwurzel ξ setzt, so hat man die Congruenz:

$$F(\xi) + \alpha^{-h} F(\xi\alpha) + \alpha^{-2h} F(\xi\alpha^2) + \ldots + \alpha^{-(\lambda-1)h} F(\xi\alpha^{-1})$$
$$\equiv \lambda A_h \xi^h, \quad \text{mod. } \phi(\alpha).$$

Wenn nun die complexen Zahlen $F(\xi)$, $F(\xi\alpha)$, $F(\xi\alpha^2)$ .... alle durch $\phi(\alpha)$ theilbar sind, so mufs nothwendig $A_h \equiv 0$ sein, nach dem Modul $\phi(\alpha)$, für alle Werthe $h = 0, 1, 2, \ldots \lambda - 1$, also alle Coefficienten von $F(w)$ müssen durch $\phi(\alpha)$ theilbar sein. Man hat daher folgenden Satz:

(V.) Wenn die complexe Zahl $F(w)$ die Eigenschaft hat, dafs alle die complexen Zahlen in α, welche man aus ihr erhält, indem man für w die λ entsprechenden Congruenzwurzeln setzt, den Faktor $\phi(\alpha)$ enthalten, so enthält $F(w)$ selbst den Faktor $\phi(\alpha)$.

§. 4.

Die idealen Primfaktoren der complexen Zahlen in w und in z.

Bei der Untersuchung der idealen Primfaktoren der complexen Zahlen in w hat man von den complexen Primzahlen in α auszugehen, welche innerhalb dieser niederen Theorie selbst ideal oder wirklich sein können, und man hat diese mit Hülfe der Wurzeln der Gleichung $w^\lambda = D(\alpha)$ weiter in diejenigen Faktoren zu zerlegen, welche innerhalb dieser höheren Theorie der complexen Zahlen in w als die wahren Primfaktoren anzusehen sind; denn die complexen Zahlen in w stehen zu denen in α genau in demselben Verhältnifs, wie diese selbst zu den gewöhnlichen ganzen Zahlen stehen: was in der niederen Theorie nothwendig als Primzahl angesehen werden mufs, wird in der höheren Theorie im Allgemeinen weiter zerlegbar, sei es in wirklicher oder in idealer Weise. Wenn also $\phi(\alpha)$ eine wirkliche oder ideale complexe Primzahl in der Theorie der complexen Zahlen in α ist, so handelt es sich darum von dem Standpunkte der Theorie der complexen Zahlen in w aus, diese Zahl $\phi(\alpha)$ weiter in diejenigen idealen oder wirklichen Faktoren zu zerlegen, welche innerhalb dieser höheren Theorie als die Primfaktoren anzusehen sind. Wenn nur diejenigen Primzahlen $\phi(\alpha)$ in Betracht gezogen werden, welche in $\varrho D(\alpha)$ nicht enthalten sind, so sind dieselben wieder in der Rücksicht besonders zu betrachten: ob für sie die Determinante $D(\alpha)$ Nichtrest oder Rest einer λten Potenz ist.

Ich stelle nun zunächst für diese beiden verschiedenen Arten der Primzahlen $\phi(\alpha)$ die Definitionen der idealen Primfaktoren innerhalb der Theorie der complexen Zahlen in w fest, und werde alsdann zeigen, dafs die so definirten idealen Primfaktoren die wesentliche und erschöpfende Eigenschaft wahrer Primfaktoren besitzen, nämlich die, dafs sie in einer jeden gegebenen complexen Zahl stets in unveränderlicher Weise enthalten sind, und dafs sie in allen Fällen, wo wirkliche Primfaktoren existiren, mit diesen vollständig übereinstimmen.

Definition: Wenn $\phi(\alpha)$ eine ideale oder wirkliche complexe Primzahl innerhalb der Theorie der complexen Zahlen in α ist, für welche $D(\alpha)$ ein Nichtrest einer λten Potenz ist, so soll $\phi(\alpha)$ auch in der Theorie der complexen Zahlen in w als Primzahl angesehen werden.

Für die Zerlegung der complexen Primzahlen der anderen Art, für welche $D(\alpha)$ ein λter Potenzrest ist, benutze ich folgende complexe Zahl:

$$(1.) \qquad \Psi(w) = (w - \xi\alpha)(w - \xi\alpha^2) \ldots\ldots (w - \xi\alpha^{\lambda-1}),$$

in welcher ξ ebenso wie oben eine Wurzel der Congruenz $\xi^\lambda \equiv D(\alpha)$, mod. $\phi(\alpha)$, bezeichnet. Diese complexe Zahl kann auch so dargestellt werden:

$$(2.) \qquad \Psi(w) = w^{\lambda-1} + \xi w^{\lambda-2} + \xi^2 w^{\lambda-3} + \ldots\ldots \xi^{\lambda-1},$$

oder in Form eines Bruches:

$$\Psi(w) = \frac{w^\lambda - \xi^\lambda}{w - \xi}.$$

Mit Hülfe dieser complexen Zahl $\Psi(w)$ gebe ich nun folgende Definition der idealen Primfaktoren des $\phi(\alpha)$ in der Theorie der complexen Zahlen in w:

Definition: Wenn $\phi(\alpha)$ eine ideale oder wirkliche complexe Primzahl innerhalb der Theorie der complexen Zahlen in α ist, für welche $D(\alpha)$ ein λter Potenzrest ist, und man hat

$$\Psi(w\alpha^{-t}) F(w) \equiv 0, \text{ mod. } \phi(\alpha),$$

so soll von $F(w)$ ausgesagt werden: es enthält einen idealen Primfaktor des $\phi(\alpha)$ und zwar denjenigen, welcher zur Congruenzwurzel $\xi\alpha^t$ gehört. Wenn ferner

$$\Psi(w\alpha^{-t})^m \cdot F(w) \equiv 0, \quad \text{mod. } \phi(\alpha)^m,$$

aber

$$\Psi(w\alpha^{-t})^{m+1} \cdot F(w) \text{ nicht} \equiv 0, \quad \text{mod. } \phi(\alpha)^{m+1},$$

so soll von der complexen Zahl $F(w)$ ausgesagt werden: sie enthält den zur Congruenzwurzel $\xi\alpha^t$ gehörenden idealen Primfaktor des $\phi(\alpha)$ genau m mal.

Nach dieser Definition giebt es in der Theorie der complexen Zahlen in w so viele verschiedene ideale Primfaktoren einer complexen Primzahl $\phi(\alpha)$ der niederen Theorie, für welche die Determinante $D(\alpha)$ ein λter Potenzrest ist, als die Congruenz

$$\xi^\lambda \equiv D(\alpha), \quad \text{mod. } \phi(\alpha)$$

verschiedene Wurzeln hat, also λ, welche als conjugirte ideale Primfaktoren des $\phi(\alpha)$ bezeichnet werden sollen, und deren Produkt, die Norm des

idealen Primfaktors, überall der Primzahl $\phi(\alpha)$ selbst gleich genommen werden soll.

Ich beweise nun zunächst, dafs die so definirten idealen Primfaktoren der folgenden ersten Bedingung wahrer Primzahlen genügen:

(I.) Wenn zwei oder mehrere complexe Zahlen einen bestimmten idealen Primfaktor nicht enthalten, so enthält das Produkt derselben diesen Primfaktor ebenfalls nicht.

Es seien $F(w)$ und $G(w)$ zwei complexe Zahlen und $H(w)$ das Produkt derselben, also $F(w) \cdot G(w) = H(w)$. Es sei ferner zunächst $\phi(\alpha)$ eine complexe Primzahl der ersten Art, für welche $D(\alpha)$ Nichtrest ist, so ist nach der Definition $\phi(\alpha)$ selbst auch in der Theorie der complexen Zahlen in w eine Primzahl. Wenn nun $F(w)$ und $G(w)$ den Faktor $\phi(\alpha)$ nicht enthalten, so enthalten nach dem zweiten der im §. 3. bewiesenen Sätze $NF(w)$ und $NG(w)$ denselben ebenfalls nicht, und weil diese Normen nur complexe Zahlen in α sind, so enthält das Produkt derselben $NF(w) \cdot NG(w) = NH(w)$ diesen Primfaktor $\phi(\alpha)$ auch nicht, woraus nach demselben erwähnten Satze des §. 3. folgt, dafs auch $H(w)$ denselben nicht enthält. Es sei nun zweitens $\phi(\alpha)$ eine Primzahl der zweiten Art, für welche $D(\alpha)$ ein λter Potenzrest ist, und $F(w)$ so wie $G(w)$ enthalten den zur Congruenzwurzel $\xi\alpha^{k}$ gehörenden idealen Primfaktor des $\phi(\alpha)$ nicht, so hat man nach der Definition

$$\begin{rcases} \Psi(w\alpha^{-k})\, F(w) \text{ nicht} \equiv 0, \\ \Psi(w\alpha^{-k})\, G(w) \text{ nicht} \equiv 0, \end{rcases} \text{mod. } \phi(\alpha).$$

Wenn nun eine complexe Zahl in w durch $\phi(\alpha)$ nicht theilbar ist, so mufs dieselbe nach dem letzten Satze des §. 3., wenn man anstatt w die Congruenzwurzeln $\xi, \xi\alpha, \xi\alpha^{2}, \ldots\, \xi\alpha^{\lambda-1}$ setzt, wenigstens für einen dieser Werthe durch $\phi(\alpha)$ nicht theilbar sein; da aber $\Psi(w)$, wie der Produktausdruck dieser complexen Zahl zeigt, congruent Null wird, sobald für w eine der Congruenzwurzeln $\xi\alpha, \xi\alpha^{2}, \ldots\, \xi\alpha^{\lambda-1}$ gesetzt wird, und nur für die eine Substitution der Congruenzwurzel ξ nicht congruent Null ist, nach dem Modul $\phi(\alpha)$, so folgt, dafs die beiden complexen Zahlen

$$\Psi(w\alpha^{-k})\, F(w) \quad \text{und} \quad \Psi(w\alpha^{-k})\, G(w)$$

für die Substitution der Congruenzwurzel $\xi\alpha^{k}$ anstatt w, nicht congruent Null werden, nach dem Modul $\phi(\alpha)$. Es ist also

$$\begin{array}{l}\Psi(\xi)\,F(\xi\alpha^{t})\ \text{nicht} \equiv 0,\\ \Psi(\xi)\,G(\xi\alpha^{t})\ \text{nicht} \equiv 0,\end{array}\quad \text{mod. } \phi(\alpha),$$

also auch

$$F(\xi\alpha^{t})\ \text{nicht} \equiv 0,\quad G(\xi\alpha^{t})\ \text{nicht} \equiv 0,\ \text{mod. } \phi(\alpha),$$

und weil diese nur complexe Zahlen in α sind, so ist auch

$$F(\xi\alpha^{t})\,G(\xi\alpha^{t})\ \text{nicht} \equiv 0,\ \text{mod. } \phi(\alpha).$$

Enthielte nun aber $F(w)\,G(w) = H(w)$ den idealen Primfaktor des $\phi(\alpha)$ welcher zur Congruenzwurzel $\xi\alpha^{t}$ gehört, so müfste nach der Definition sein:

$$\Psi(w\alpha^{-t})\,F(w)\,G(w) \equiv 0,\ \text{mod. } \phi(\alpha),$$

also, wenn für w die Congruenzwurzel $\xi\alpha^{t}$ gesetzt wird, so müfste auch

$$\Psi(\xi)\,F(\xi\alpha^{t})\,G(\xi\alpha^{t}) \equiv 0,\ \text{mod. } \phi(\alpha),$$

sein, und weil $\Psi(\xi)$ nicht congruent Null ist, so müfste

$$F(\xi\alpha^{t})\,G(\xi\alpha^{t}) \equiv 0,\ \text{mod. } \phi(\alpha)$$

sein, welches nicht der Fall ist. Das Produkt $F(w)\,G(w) = H(w)$ enthält also keinen idealen Primfaktor, welcher nicht schon in einem der beiden Faktoren enthalten ist, und dieser für das Produkt zweier Faktoren bewiesene Satz wird ohne Schwierigkeit auch auf jedes Produkt einer beliebigen Anzahl von Faktoren ausgedehnt.

Auf diesen soeben bewiesenen specielleren Satz stützt sich nun der Beweis des folgenden allgemeineren Satzes:

(II.) Das entwickelte Produkt zweier oder mehrerer complexer Zahlen in w enthält genau dieselben idealen Primfaktoren, und zwar jeden derselben genau so oft, als die Faktoren dieses Produkts zusammengenommen.

Es sei wieder $F(w)\,G(w) = H(w)$, und es sei erstens $\phi(\alpha)$ eine complexe Primzahl der ersten Art, für welche $D(\alpha)$ Nichtrest einer λten Potenz ist, welche also auch in der Theorie der complexen Zahlen in w als Primzahl definirt ist. Diese Primzahl $\phi(\alpha)$ sei in $F(w)$ genau m mal und in $G(w)$ genau n mal enthalten, so dafs man setzen kann:

$$F(w) = \phi(\alpha)^{m}\,F_{1}(w),\quad G(w) = \phi(\alpha)^{n}\,G_{1}(w),$$

so ist

$$H(w) = \phi(\alpha)^{m+n}\,F_{1}(w)\,G_{1}(w),$$

also $H(w)$ enthält den Primfaktor $\phi(\alpha)$ $m+n$ mal. Dafs es denselben auch nicht mehr als $m+n$ mal enthält, folgt aber daraus, dafs weder $F_1(w)$ noch $G_1(w)$ denselben enthält, und folglich nach dem vorigen Satze auch das Produkt $F_1(w)\ G_1(w)$ ihn nicht enthalten kann.

Es sei nun zweitens $\phi(\alpha)$ eine complexe Primzahl der zweiten Art, für welche $D(\alpha)$ ein λter Potenzrest ist, und es enthalte $F(w)$ den zur Congruenzwurzel $\xi\alpha^t$ gehörenden idealen Primfaktor des $F(\alpha)$ genau m mal, $G(w)$ enthalte denselben genau n mal, so hat man:

$$\Psi(w\alpha^{-t})^m F(w) \equiv 0 \text{ mod. } \phi(\alpha)^m,$$
$$\Psi(w\alpha^{-t})^n G(w) \equiv 0 \text{ mod. } \phi(\alpha)^n,$$

also kann man setzen:

$$\Psi(w\alpha^{-t})^m F(w) = \phi(\alpha)^m P(w),$$
$$\Psi(w\alpha^{-t})^n G(w) = \phi(\alpha)^n Q(w),$$

woraus folgt:

$$\Psi(w\alpha^{-t})^{m+n} F(w)\ G(w) = \phi(\alpha)^{m+n} P(w)\ Q(w),$$

Diese Gleichung zeigt, dafs das Produkt $F(w)\ G(w) = H(w)$ den zur Congruenzwurzel $\xi\alpha^t$ gehörenden idealen Primfaktor des $\phi(\alpha)$ $m+n$ mal enthält. Dafs es denselben auch nicht mehr als $m+n$ mal enthält, wird folgendermaafsen bewiesen. Nach der Voraussetzung, dafs $F(w)$ den in Rede stehenden idealen Primfaktor nicht mehr als m mal, und $G(w)$ denselben nicht mehr als n mal enthält, hat man:

$$\Psi(w\alpha^{-t})^{m+1} F(w) \text{ nicht} \equiv 0, \text{ mod. } \phi(\alpha)^{m+1},$$
$$\Psi(w\alpha^{-t})^{n+1} G(w) \text{ nicht} \equiv 0, \text{ mod. } \phi(\alpha)^{n+1},$$

also

$$\Psi(w\alpha^{-t})\ \phi(\alpha)^m P(w) \text{ nicht} \equiv 0, \text{ mod. } \phi(\alpha)^{m+1},$$
$$\Psi(w\alpha^{-t})\ \phi(\alpha)^n Q(w) \text{ nicht} \equiv 0, \text{ mod. } \phi(\alpha)^{n+1},$$

und folglich auch:

$$\Psi(w\alpha^{-t})\ P(w) \text{ nicht} \equiv 0, \text{ mod. } \phi(\alpha),$$
$$\Psi(w\alpha^{-t})\ Q(w) \text{ nicht} \equiv 0, \text{ mod. } \phi(\alpha),$$

woraus folgt, dafs weder $P(w)$ noch $Q(w)$ diesen idealen Primfaktor enthält, und mithin das Produkt derselben ihn ebenfalls nicht enthalten kann, oder was dasselbe ist, dafs das Produkt

$$\Psi(w\alpha^{-k})\,P(w)\,Q(w)$$

den Faktor $\phi(\alpha)$ nicht enthalten kann. Aus der Gleichung

$$\Psi(w\alpha^{-k})^{m+n}\,F(w)\,G(w) = \phi(\alpha)^{m+n}\,P(w)\,Q(w)$$

folgt aber:

$$\Psi(w\alpha^{-k})^{m+n+1}\,F(w)\,G(w) = \phi(\alpha)^{m+n}\,\Psi(w\alpha^{-k})\,P(w)\,Q(w),$$

und hieraus:

$$\Psi(w\alpha^{-k})^{m+n+1}\,F(w)\,G(w) \text{ nicht} \equiv 0, \text{ mod. } \phi(\alpha)^{m+n+1};$$

also das Produkt $F(w)\,G(w)$ enthält den zur Congruenzwurzel $\xi\alpha^{k}$ gehörenden idealen Primfaktor des $\phi(\alpha)$ nicht mehr als $m+n$ mal. Eine wiederholte Anwendung dieses für zwei Faktoren bewiesenen Satzes zeigt, dafs derselbe ebenso für ein Produkt beliebig vieler Faktoren gültig ist.

§. 5.

Verhältnifs der idealen complexen Zahlen zu den wirklichen.

Der in dem vorhergehenden Paragraphen bewiesene Hauptsatz zeigt, dafs die idealen Primfaktoren, wie sie oben definirt sind, die erste Grundeigenschaft wahrer Primfaktoren haben, nämlich in einer und derselben Zahl in unveränderlicher Weise enthalten zu sein, und unabhängig davon, ob diese Zahl in entwickelter Form, oder in Form eines Produkts gegeben ist. Es sind nun weiter diejenigen Sätze zu entwickeln, welche die Übereinstimmung dieser idealen Primfaktoren mit den wirklichen, wo solche existiren, nachweisen, und welche zeigen, welchen Gebrauch man von den idealen Primfaktoren, vorzüglich in der Multiplikation und Division der complexen Zahlen in w machen kann.

(I.) **Wenn eine complexe Zahl $F(w)$ alle λ idealen Primfaktoren einer Primzahl $\phi(\alpha)$ enthält, für welche die Determinante $D(\alpha)$ ein λter Potenzrest ist, und zwar jeden derselben mindestens m mal, so ist $F(w)$ durch $\phi(\alpha)^m$ theilbar.**

Nach der Voraussetzung dieses Satzes hat man nämlich:

$$\Psi(w\alpha^{-k})^m F(w) \equiv 0, \quad \text{mod. } \phi(\alpha)^m,$$

für alle Werthe des $k = 0, 1, 2, \ldots \lambda - 1$. Giebt man nun dem k nach einander alle diese λ Werthe und summirt, so erhält man:

$$\left(\Psi(w)^m + \Psi(w\alpha^{-1})^m + \ldots. + \Psi(w\alpha^{-(\lambda-1)})^m\right) F(w) \equiv 0, \text{ mod. } \phi(\alpha)^m.$$

Die Summe innerhalb der Klammern, als symmetrische Funktion aller Wurzeln der Gleichung $w^\lambda = D(\alpha)$, enthält die Wurzel w selbst nicht, und ist nur eine complexe Zahl in α, welche durch $\Phi(\alpha)$ bezeichnet werden mag. Nimmt man nun $F(w)$ in der Form

$$F(w) = A + A_1 w + A_2 w^2 + \ldots. + A_{\lambda-1} w^{\lambda-1},$$

so hat man:

$$\Phi(\alpha)\,(A + A_1 w + A_2 w^2 + \ldots. + A_{\lambda-1} w^{\lambda-1}) \equiv 0, \text{ mod. } \phi(\alpha)^m.$$

Vermöge der Irreductibilität der Gleichung $w^\lambda = D(\alpha)$ kann aber diese Congruenz nicht bestehen, ohne dafs folgende λ einzelnen Congruenzen Statt haben:

$$\Phi(\alpha)\,A \equiv 0,\ \Phi(\alpha)\,A_1 \equiv 0,\ \ldots.,\ \Phi(\alpha)\,A_{\lambda-1} \equiv 0, \text{ mod. } \phi(\alpha)^m.$$

$\Phi(\alpha)$ aber enthält den Faktor $\phi(\alpha)$ nicht; denn wenn man in der Gleichung

$$\Phi(\alpha) = \Psi(w)^m + \Psi(w\alpha^{-1})^m + \ldots. + \Psi(w\alpha^{-(\lambda-1)})^m$$

die Wurzel w durch die Congruenzwurzel ξ ersetzt, und bemerkt, dafs die in der Gleichung (2.) §. 4. gegebene Form des $\Psi(w)$

$$\Psi(\xi\alpha^{-h}) \equiv \xi^{\lambda-1}\,(\alpha^h + \alpha^{2h} + \alpha^{3h} + \ldots. + \alpha^{(\lambda-1)h} + 1), \text{ mod. } \phi(\alpha),$$

ergiebt, also allgemein:

$$\Psi(\xi\alpha^{-h}) \equiv 0, \text{ mod. } \phi(\alpha), \text{ wenn } h \text{ nicht} = 0,$$

aber für $h = 0$:

$$\Psi(\xi) \equiv \lambda\xi^{\lambda-1}, \text{ mod. } \phi(\alpha),$$

so hat man:

$$\Phi(\alpha) \equiv \lambda^m\,\xi^{(\lambda-1)m}, \text{ mod. } \phi(\alpha);$$

also $\Phi(\alpha)$ nicht durch $\phi(\alpha)$ theilbar. Hieraus folgt, dafs die Coefficienten

$A, A_1, A_2, \ldots A_{\lambda-1}$ alle einzeln den Faktor $\phi(a)^m$ enthalten müssen, dafs also $F(w)$ durch $\phi(a)^m$ theilbar sein mufs, w. z. b. w.

(II.) Wenn eine complexe Zahl $F(w)$ genau m ideale Primfaktoren einer Primzahl $\phi(a)$ enthält, für welche die Determinante $D(a)$ ein λter Potenzrest ist, dieselben mögen verschieden sein, oder auch nicht, so enthält die Norm von $F(w)$ den Faktor $\phi(a)$ genau m mal.

Die Norm $NF(w)$, als das Produkt der λ conjugirten complexen Zahlen, mufs nach der Voraussetzung des Satzes jeden der λ verschiedenen idealen Primfaktoren des $\phi(w)$ genau m mal enthalten; also mufs sie, vermöge des vorigen Satzes, den Faktor $\phi(a)^m$ enthalten. Dieselbe kann auch nicht eine höhere Potenz von $\phi(a)$ enthalten, weil sie sonst einen jeden der λ idealen Primfaktoren des $\phi(a)$ mehr als m mal enthalten müfste.

Dieser Lehrsatz, verbunden mit dem Lehrsatz II. §. 3., zeigt nicht nur, dafs die Anzahl der in einer gegebenen complexen Zahl $F(w)$ enthaltenen idealen Primfaktoren stets eine endliche bestimmte ist, sondern er gewährt auch ein leichtes Mittel um zu erkennen, wie viele ideale Primfaktoren dieselbe enthält, und von welchen Primzahlen in der niederen Theorie der complexen Zahlen in a sie herrühren. Bildet man nämlich die Norm $NF(w)$, zerlegt dieselbe als complexe Zahl in a in ihre, dieser niederen Theorie angehörenden Primfaktoren, und unterscheidet dabei diejenigen Primfaktoren, für welche die Determinante Nichtrest einer λten Potenz ist, von denen, wo sie Rest ist: so mufs erstens die Anzahl, wie viel mal eine solche Primzahl der ersten Art in $NF(w)$ vorkommt, ein Vielfaches von λ sein, und wenn dieselbe gleich $k\lambda$ ist, so ist dieser ideale Primfaktor, welcher in der höheren Theorie ebenfalls Primfaktor ist, genau k mal in $F(w)$ enthalten; wenn zweitens irgend eine Primzahl der zweiten Art genau m mal in der Norm vorkommt, so mufs $F(w)$ selbst nothwendig m ideale Primfaktoren derselben in der höheren Theorie der complexen Zahlen in w enthalten. Die Norm $NF(w)$ kann aufserdem noch Primfaktoren der Determinante $D(a)$, oder auch den Primfaktor $1-a$ enthalten, von deren zugehörenden idealen Primfaktoren in der Theorie der complexen Zahlen in w aber erst weiter unten die Rede sein wird.

(III.) Wenn $f(w)$ eine wirkliche complexe Zahl in w ist, deren Norm keinen gemeinschaftlichen Faktor mit $\varrho D(a)$ hat,

und $F(w)$ eine andere wirkliche complexe Zahl in w, welche alle idealen Primfaktoren des $f(w)$, jeden mindestens eben so oft, als $f(w)$ selbst enthält, so ist $F(w)$ durch $f(w)$ theilbar.

Man kann den Quotienten der beiden Zahlen $F(w)$ und $f(w)$ in folgende Form setzen:

$$\frac{F(w)}{f(w)} = \frac{F(w) \, . \, f(w\alpha) \, f(w\alpha^2) \, ... \, f(w\alpha^{\lambda-1})}{Nf(w)} \, .$$

Wenn nun erstens $f(w)$ irgend einen Primfaktor $\phi(\alpha)$ n mal enthält, für welchen $D(\alpha)$ Nichtrest ist, welcher also in der niederen und in der höheren Theorie zugleich Primfaktor ist, so kommt derselbe in dem Nenner $Nf(w)$ nothwendig $n\lambda$ mal vor, und eben so viel mal mindestens kommt er auch in dem Zähler vor, weil jede der complexen Zahlen $f(w\alpha)$, $f(w\alpha^2)$, ... $f(w\alpha^{\lambda-1})$ denselben genau n mal, und $F(w)$ denselben nach der Voraussetzung des Satzes mindestens n mal enthält. Jeder solcher Faktor hebt sich also aus dem Nenner des Bruches vollständig hinweg. Wenn nun zweitens $f(w)$ irgend welche idealen Primfaktoren einer Primzahl der niederen Theorie $\phi(\alpha)$ enthält, für welche $D(\alpha)$ Rest einer λten Potenz ist, und die Anzahl dieser idealen Primfaktoren ist m, so enthält der Nenner $Nf(w)$ den Faktor $\phi(\alpha)$ genau m mal, der Zähler $F(w) \, f(w\alpha) \, f(w\alpha^2) \, ... \, f(w\alpha^{\lambda-1})$ enthält aber alle idealen Primfaktoren des $\phi(\alpha)$, jeden mindestens m mal, weil $F(w)$ alle idealen Primfaktoren des $f(w)$ enthält, also vermöge des Satzes (II.) enthält der Zähler den Faktor $\phi(\alpha)$ nothwendig m mal, also auch ein jeder solcher Faktor mufs sich vollständig aus dem Nenner hinwegheben. Da endlich in $Nf(w)$ nach der Voraussetzung des Satzes keine anderen, als die hier untersuchten Faktoren vorkommen, indem die in $\varrho D(\alpha)$ enthaltenen ausgeschlossen sind, so folgt, dafs der ganze Nenner $Nf(w)$ gegen den Zähler sich hinwegheben mufs, und dafs der Quotient $\frac{F(w)}{f(w)}$ eine **ganze** complexe Zahhl ist, w. z. b. w.

(IV.) **Wenn zwei wirkliche complexe Zahlen in w genau dieselben idealen Primfaktoren enthalten, und wenn ihre Normen keinen gemeinschaftlichen Faktor mit $\varrho D(\alpha)$ haben, so unterscheiden sich diese Zahlen nur durch Einheiten, welche als Faktoren hinzutreten können.**

Die beiden wirklichen complexen Zahlen, von denen der Satz handelt, seien $F(w)$ und $f(w)$, so ist vermöge des vorhergehenden Satzes:

$$\frac{F(w)}{f(w)} = E(w),\quad F(w) = E(w)\,f(w),$$

wo $E(w)$ eine ganze complexe Zahl ist, und zwar eine wirkliche. Nimmt man nun auf beiden Seiten die Normen, so hat man:

$$NF(w) = NE(w) \cdot Nf(w).$$

Die beiden Normen $NF(w)$ und $Nf(w)$, welche complexe Zahlen in α sind, enthalten nun genau dieselben Primfaktoren, auch in dieser niederen Theorie. Dieselben können sich daher nur durch eine Einheit $E(\alpha)$ unterscheiden, und man hat:

$$NF(w) = E(\alpha)\,Nf(w),$$

und diese Gleichung, mit der vorhergehenden verbunden, ergiebt:

$$NE(w) = E(\alpha).$$

Die ganze complexe Zahl $E(w)$ ist also eine solche, deren Norm eine Einheit in α ist, sie ist daher eine Einheit in der Theorie der complexen Zahlen in w, weil überhaupt als Einheit in dieser Theorie eine jede ganze complexe Zahl, deren Norm eine Einheit der niederen Theorie der complexen Zahlen in α ist, definirt wird.

Aus den hier angenommenen Resultaten ergiebt sich nun leicht der Satz, welcher noch erfordert wird, um die gegebenen Definitionen der idealen Primfaktoren zu rechtfertigen, nämlich:

(V.) In jedem Falle, wo in der Theorie der complexen Zahlen in w ein Primfaktor einer Primzahl $\phi(\alpha)$ der niederen Theorie, für welche $D(\alpha)$ ein λter Potenzrest ist, als ein wirklicher existirt, und darum als eine complexe Zahl in w definirt werden kann, deren Norm, abgesehen von einer Einheit, gleich $\phi(\alpha)$ ist, stimmt die oben gegebene allgemeine Definition vollständig mit dieser beschränkteren zusammen.

Es sei $f(w)$ ein wirklicher complexer Primfaktor der Primzahl $\phi(\alpha)$ der niederen Theorie, also $Nf(w) = E(\alpha)\,\phi(\alpha)$, wo $E(\alpha)$ eine Einheit ist, so mufs für eine bestimmte Wurzel der Congruenz $\xi^\lambda \equiv D(\alpha)$, mod. $\phi(\alpha)$, welche statt w gesetzt wird, z. B. für die Wurzel $\xi\alpha^k$, wie oben §. 3. bewiesen worden, $f(\xi\alpha^k) \equiv 0$, mod. $\phi(\alpha)$, sein, und es ist alsdann $f(w)$ als der zur Congruenzwurzel $\xi\alpha^k$ gehörende Primfaktor des $\phi(\alpha)$ zu bezeichnen.

Wenn nun eine wirkliche complexe Zahl $F(w)$ alle idealen Primfaktoren des $f(w)$, im vorliegenden Falle also nur den einen zur Congruenzwurzel $\xi \alpha^k$ gehörenden Primfaktor des $\phi(\alpha)$ enthält, so ist, wie oben gezeigt worden, $F(w)$ durch $f(w)$ theilbar, also:

$$\frac{F(w)}{f(w)} = G(w) \text{ oder } F(w) = f(w)\, G(w),$$

wo $G(w)$ eine ganze und wirkliche complexe Zahl ist. Der in $F(w)$ enthaltene ideale Primfaktor tritt also in diesem Falle als der wirkliche heraus.

Es würde jetzt eigentlich noch übrig sein, auch von den idealen Primfaktoren derjenigen complexen Primzahlen in α zu handeln, welche in der Determinante $D(\alpha)$ enthalten sind, so wie über die Zerlegung von $1 - \alpha = \varrho$ in der höheren Theorie der complexen Zahlen in w. Es treten aber bei der Zerlegung dieser Primzahlen in einfachere Faktoren der höheren Theorie ganz eigenthümliche Umstände ein, welche bewirken, dafs es im Allgemeinen unmöglich ist, wahre ideale Primfaktoren der in $\varrho D(\alpha)$ enthaltenen complexen Primzahlen anzugeben, welche im vollen Sinne diesen Namen verdienen, so wie die hier behandelten; namentlich treten diese störenden Umstände immer dann ein, wenn ein Primfaktor mehr als einmal in der Determinante enthalten ist. Für den vorliegenden Zweck ist es aber nicht nöthig, die Zerlegung der in $\varrho D(\alpha)$ enthaltenen Faktoren der niederen Theorie in die idealen Faktoren, welche sie innerhalb der höheren Theorie der complexen Zahlen in w haben möchten, näher zu untersuchen. Der Ausdruck „idealer Primfaktor" oder „ideale Primzahl" dieser höheren Theorie, wird darum überall nur von den im §. 4. definirten idealen Primfaktoren gebraucht werden, deren Normen ausschliefslich nur die in $\varrho D(\alpha)$ nicht enthaltenen Primzahlen der niederen Theorie sind. Ebenso soll auch der Ausdruck „ideale complexe Zahl" in der höheren Theorie nur von einer Zusammensetzung der definirten idealen Primfaktoren gebraucht werden, d. h. von dem gleichzeitigen Bestehen beliebig vieler, der die idealen Primfaktoren charakterisirenden Congruenzbedingungen, oder von dem Bestehen einer derjenigen Congruenzbedingungen, welche ausdrücken, dafs eine complexe Zahl einen idealen Primfaktor mehrmals enthält, niemals aber soll von idealen Zahlen die Rede sein, deren Normen irgend welche Faktoren mit $\varrho D(\alpha)$ gemein haben möchten. Dadurch soll jedoch die Anwendung wirklicher complexer Zahlen in w oder z nicht ausgeschlossen werden, deren

Normen den Faktor ϱ oder Primfaktoren der Determinante $D(\alpha)$ enthalten, von denen vielmehr in dem Folgenden mit grofsem Nutzen Gebrauch gemacht werden wird.

§. 6.

Eintheilung der idealen complexen Zahlen in die Klassen und Bestimmung der Klassenanzahl.

Die idealen Primfaktoren der complexen Zahlen in w, welche in den vorhergehenden beiden Paragraphen durch Congruenzbedingungen definirt und in ihren wesentlichen Grundeigenschaften betrachtet worden sind, bleiben vollkommen dieselben, wenn man die speciellere Theorie der complexen Zahlen in z zu Grunde legt, denn jede ganze complexe Zahl in z ist zugleich auch eine ganze complexe Zahl in w. Die Definition der Aequivalenz, nach welcher zwei ideale Zahlen äquivalent heifsen, wenn sie mit einer und derselben dritten idealen Zahl zusammengesetzt, wirkliche complexe Zahlen ergeben, so wie die allgemeinen Sätze über Zusammensetzung, Aequivalenz und Klassifikation der idealen Zahlen, sind sogar nicht nur für die beiden Arten der complexen Zahlen in z und in w, sondern für die idealen Zahlen aller complexen Theorieen, welche überhaupt existiren, vollständig dieselben. Es sind diefs die Sätze, welche ich im §. 5. meines *Memoire sur la théorie des nombres complexes* etc. in Liouville's Journal, Bd. 16, pg. 439 etc. von den aus λten Wurzeln der Einheit gebildeten, und später in einer vor der Königlichen Akademie vorgetragenen, in den Abhandlungen vom Jahre 1856 gedruckten Abhandlung, auch von den, aus beliebigen Wurzeln der Einheiten, deren Wurzelexponenten nicht Primzahlen sind, gebildeten complexen Zahlen vollständig bewiesen habe, nämlich folgende:

(I.) Es giebt stets eine endliche bestimmte Anzahl idealer Multiplikatoren, welche hinreichen, um alle idealen Zahlen zu wirklichen zu machen, wenn sie mit denselben zusammengesetzt werden, oder die Anzahl aller nichtäquivalenten Klassen der idealen Zahlen ist eine endliche bestimmte.

(II.) Die Eintheilung der nichtäquivalenten idealen Zahlen in die verschiedenen Klassen ist von der zufälligen Wahl der idealen Multiplikatoren ganz unabhängig.

(III.) Wenn zwei ideale Zahlen einer dritten äquivalent sind, so sind sie unter einander äquivalent.

(IV.) Aequivalente ideale Zahlen mit äquivalenten zusammengesetzt, geben äquivalente Produkte.

(V.) Jede ideale Zahl wird durch Erhebung zu einer bestimmten Potenz zu einer wirklichen, und kann daher als Wurzel aus einer wirklichen complexen Zahl dargestellt werden.

(VI.) Der Exponent der niedrigsten Potenz einer idealen Zahl, welche zu einer wirklichen wird, ist ein genauer Theil der Anzahl aller verschiedenen Klassen.

Die Beweise dieser Sätze für die Theorie der complexen Zahlen in w oder z will ich hier unterdrücken, da dieselben gröfstentheils fast wörtlich mit den an den angeführten Orten, für die aus Einheitswurzeln gebildeten, complexen Zahlen, gegebenen übereinstimmen würden. Nur in dem Beweise des ersten Satzes, über die endliche Anzahl der Klassen, müssen gewisse Modifikationen eintreten, welche jedoch eben so wenig neue principielle Schwierigkeiten darbieten. Ich kann in Betreff dieser, so wie überhaupt der allgemeinen Sätze, welche allen Theorieen complexer Zahlen gemein sind auch auf eine Arbeit von Hrn. Kronecker verweisen, welche nächstens erscheinen wird, in welcher die Theorie der allgemeinsten complexen Zahlen, in ihrer Verbindung mit der Theorie der zerlegbaren Formen aller Grade, vollständig und in grofsartiger Einfachheit entwickelt ist.

Man kann auch in ähnlicher Weise wie ich diefs im §. VIII der angeführten Abhandlung in Liouville's Journal, Bd. 16, pag. 454 etc. für die aus Wurzeln der Einheit gebildeten, complexen Zahlen vollständig ausgeführt habe, nach den Dirichletschen Methoden einen Ausdruck für die Klassenanzahl der complexen Zahlen in w entwickeln, und ebenso den entsprechenden für die complexen Zahlen in z. Da dieser Ausdruck für eine der folgenden Untersuchungen von Wichtigkeit ist, so will ich denselben hier in der Kürze entwickeln, indem ich mich begnüge, die Hauptmomente der Methode anzugeben, die Ausführung im Einzelnen aber, in so weit sie keinerlei Schwierigkeit hat, übergehe.

Es wird folgende Reihe zu Grunde gelegt:

$$(1.)\qquad R = (s-1)\ \Sigma\ \frac{1}{(NNF(w))^s},$$

in welcher $F(w)$ alle verschiedenen idealen Zahlen in w repräsentirt, d. h. alle, welchen verschiedene Zerlegungen in ihre Primfaktoren zukommen,

wo ferner $\dot{N}NF(w)$ die Norm von $F(w)$, zuerst in Beziehung auf w, und sodann in Beziehung auf α genommen bedeutet, und s eine Zahl > 1 ist. Die in Beziehung auf w genommene Norm von $F(w)$, als complexe Zahl in α in ihre Primfaktoren dieser niederen Theorie zerlegt, hat stets folgende Form:

$$NF(w) = \varphi(\alpha)^{m}\,\varphi_1(\alpha)^{m_1} \dots \psi(\alpha)^{n\lambda}\,\psi_1(\alpha)^{n_1\lambda} \dots$$

wo $\varphi(\alpha)$, $\varphi_1(\alpha)$ ... Primzahlen sind, für welche $D(\alpha)$ ein λter Potenzrest ist, dagegen $\psi(\alpha)$, $\psi_1(\alpha)$ solche, deren Nichtrest $D(\alpha)$ ist. Es giebt nun genau

$$\frac{\lambda(\lambda+1)\dots(\lambda+m-1)}{1.\,2.\,\dots\,m}\cdot\frac{\lambda(\lambda+1)\dots(\lambda+m_1-1)}{1.\,2.\,\dots\,m_1}\dots\dots$$

verschiedene ideale Zahlen $F(w)$, welche diese selbe Norm haben, weil jede der Zahlen $\varphi(\alpha)$ λ verschiedene ideale Primfaktoren hat, jede der Zahlen $\psi(\alpha)$ aber auch in der höheren Theorie selber Primzahl ist, also $\varphi(\alpha)^m$ auf so viele Weisen entstehen kann, als man die λ idealen Primfaktoren des $\varphi(\alpha)$ mit Wiederholungen, aber ohne Versetzungen zu je m verbinden kann, $\psi(\alpha)^n$ aber nur auf eine Weise entstehen kann. Demnach ist:

$$(2.)\qquad R = (s-1)\,\Sigma\,\frac{\dfrac{\lambda(\lambda+1)\dots(\lambda+m-1)}{1.\,2.\,\dots\,m}\cdot\dfrac{\lambda(\lambda+1)\dots(\lambda+m_1-1)}{1.\,2.\,\dots\,m_1}\dots}{N\varphi(\alpha)^{ms}\,N\varphi_1(\alpha)^{m_1 s}\dots N\psi(\alpha)^{n\lambda s}\,N\psi_1(\alpha)^{n_1\lambda s}\dots},$$

wo die Summe auf alle ganzzahligen Werthe der Gröfsen m, m_1 ... n, n_1 ... von Null bis Unendlich sich bezieht. Führt man diese einzelnen Summationen nach dem binomischen Lehrsatze aus, so erhält man:

$$(3.)\qquad R = (s-1)\left(1-\frac{1}{N\varphi(\alpha)^s}\right)^{-\lambda}\cdot\left(1-\frac{1}{N\varphi_1(\alpha)^s}\right)^{-\lambda}\dots\left(1-\frac{1}{N\psi(\alpha)^{\lambda s}}\right)^{-1}\dots$$

Die beiden verschiedenen Arten der Faktoren dieses Produkts werden mit Hülfe des Legendreschen Zeichens $\left(\frac{D(\alpha)}{\varphi(\alpha)}\right)$ leicht unter eine und dieselbe Form gebracht, denn das Produkt

$$\prod_{0}^{\lambda-1}{}_k\left(1-\frac{\left(\frac{D(\alpha)}{\varphi(\alpha)}\right)^k}{N\varphi(\alpha)^s}\right)^{-1}$$

giebt, wenn $D(\alpha)$ Rest von $\varphi(\alpha)$ ist, einen Faktor der ersten Art, und wenn $D(\alpha)$ Nichtrest von $\varphi(\alpha)$ ist, einen Faktor der zweiten Art. Man erhält so,

wenn der Kürze wegen das auf alle idealen Primzahlen in α, mit Ausschlufs der in $\varrho D(\alpha)$ enthaltenen, bezogene unendliche Produkt:

$$(4.)\qquad \Pi\left(1-\frac{\left(\frac{D(\alpha)}{\phi(\alpha)}\right)^k}{N\phi(\alpha)^s}\right)^{-1} = L_k$$

gesetzt wird:

$$(5.)\qquad R = (s-1)\, L_0\, L_1\, L_2 \,\ldots\, L_{\lambda-1}.$$

Durch Entwickelung der (-1)ten Potenz der zweitheiligen Gröfse und Ausführung der angedeuteten Multiplikation erhält man aus dem Produktausdrucke des L_k nach bekannter Methode folgenden Summenausdruck:

$$(6.)\qquad L_k = \Sigma\,\frac{\left(\frac{D(\alpha)}{F(\alpha)}\right)^k}{NF(\alpha)^s},$$

in welchem $F(\alpha)$ alle verschiedenen idealen Zahlen in der Theorie der complexen Zahlen in α bezeichnet, welche keinen gemeinschaftlichen Faktor mit $\varrho D(\alpha)$ haben, $\left(\frac{D(\alpha)}{F(\alpha)}\right)$ das in bekannter Weise für zusammengesetzte Moduln verallgemeinerte Legendresche Zeichen ist, und das Summenzeichen auf alle verschiedenen, idealen Zahlen $F(\alpha)$ zu beziehen ist. Der Werth der Reihe $(s-1)\, L_0$, für $s=1$, jedoch mit Zulassung der idealen Zahlen $F(\alpha)$, welche mit $\varrho D(\alpha)$ gemeinschaftliche Faktoren haben, ist in meiner Abhandlung in Liouville's Journal, Bd. 16, pag. 460 gegeben, und ist, um in den Zahlen $F(\alpha)$ die mit $\varrho D(\alpha)$ gemeinschaftlichen Faktoren auszuschliefsen, wenn $D(\alpha)$ die verschiedenen Primfaktoren $f(\alpha)$, $f_1(\alpha)$, ... enthält, nur mit

$$(7.)\qquad \left(1-\frac{1}{\lambda}\right)\left(1-\frac{1}{Nf(\alpha)}\right)\left(1-\frac{1}{Nf_1(\alpha)}\right)\ldots = C$$

zu multipliciren. Man hat daher:

$$(8.)\qquad (s-1)\, L_0 = \frac{2^{\mu-1}\pi^{\mu}\, C\, P\, D}{\lambda^{2\mu-\frac{1}{2}}},\ \text{für } s=1,$$

wo $\mu=\frac{\lambda-1}{2}$, und P und D die am angeführten Orte angegebenen Bedeutungen haben, und wenn dieser gefundene Werth der Einfachheit wegen mit K bezeichnet wird:

$$(9.)\qquad R = K\, L_1\, L_2\, L_3 \,\ldots\, L_{\lambda-1},\ \text{für } s=1.$$

Es wird nun der Werth der Reihe R für den Gränzwerth $s = 1$ nach einer anderen Methode gefunden, indem diese Reihe in so viel besondere Reihen zerlegt wird, als es verschiedene Klassen der idealen Zahlen $F(w)$ giebt. Sei H die Anzahl dieser Klassen, und $F_0(w)$, $F_1(w)$, ... $F_{H-1}(w)$ bezeichnen alle idealen Zahlen beziehungsweise der ersten, zweiten u. s. w. Klasse, so ist:

$$(10.)\qquad R = \Sigma\, \frac{s-1}{NNF_0(w)^s} + \Sigma\, \frac{s-1}{NNF_1(w)^s} + \dots + \Sigma\, \frac{s-1}{NNF_{H-1}(w)^s}\,.$$

Es wird hier zunächst auf dieselbe Weise, wie in der genannten Abhandlung pag. 469 gezeigt, daſs für $s = 1$ alle diese H verschiedenen Summen denselben Werth erhalten, so daſs es hinreicht die erste derselben, in welcher $F_0(w)$ die erste Klasse, die der wirklichen complexen Zahlen in w repräsentirt, zu finden. Man kann nun jede wirkliche complexe Zahl $F_0(w)$, welche λ complexe Zahlen in α als Coefficienten hat, deren jeder wieder $\lambda - 1$ nicht-complexe Coefficienten enthält, die als unbestimmte Zahlen mit $x_{h,k}$ bezeichnet werden sollen, so darstellen:

$$(11.)\qquad F_0(w) = \sum_0^{\lambda-2}{}_h \sum_0^{\lambda-1}{}_k\; x_{h,k}\, \alpha^h\, w^k\,.$$

Für alle möglichen Werthe der ganzzahligen Coefficienten $x_{h,k}$ erhält man nun aber nicht bloſs verschiedene wirkliche complexe Zahlen $F_0(w)$, sondern auch alle diejenigen, welche sich nur durch Einheiten unterscheiden. Um in dieser Form eine jede complexe Zahl nur einmal zu haben, muſs man mit Hülfe der Fundamental-Einheiten die Coefficienten den nöthigen Beschränkungen unterwerfen. Nach Hrn. Dirichlet's Untersuchungen über die allgemeinen Einheiten, giebt es aber für die complexen Zahlen in w $\frac{\lambda(\lambda-1)}{2} - 1$ Fundamental-Einheiten, über welche weiter unten vollständig gehandelt werden wird, und wenn man dieselben durch $\varepsilon_1(w)$, $\varepsilon_2(w)$, etc. bezeichnet, so sind alle Einheiten in der Form

$$(12.)\qquad \alpha_1\, \varepsilon_1(w)^{m_1}\, \varepsilon_2(w)^{m_2} \,\dots\, \varepsilon_{\nu-1}(w)^{m_{\nu-1}}$$

enthalten, in welcher α_1 eine der $2\lambda^2$ Wurzeln der Gleichung $\alpha_1^{2\lambda^2} = 1$, $\nu = \frac{\lambda(\lambda-1)}{2}$ ist, und $m_1, m_2, \dots m_{\nu-1}$ alle möglichen positiven und negativen ganzen Zahlen sein können. Bezeichnet man nun mit $MF(w)$ und $M\varepsilon_k(w)$ die analytischen Moduln der imaginären Gröſsen $F(w)$ und $\varepsilon_k(w)$, so erhält

man in ähnlicher Weise, wie in der erwähnten Abhandlung, das Resultat: Wenn die Coefficienten $x_{k,i}$ in der complexen Zahl $F_0(w)$ so beschränkt werden, daſs in dem Systeme von Gleichungen, welches man aus der Gleichung

$$(13.)\quad \log. MF_0(w) = y_1 \log. M\varepsilon_1(w) + y_2 \log. M\varepsilon_2(w) + \dots + y_{\nu-1} \log. M\varepsilon_{\nu-1}(w)$$

erhält, indem man zu den darin enthaltenen complexen Zahlen ihre conjugirten nimmt, die Gröſsen $y_1, y_2, \dots y_{\nu-1}$ alle in den Gränzen 0 und 1 liegen müssen: so enthält die Form $F_0(w)$ alle verschiedenen wirklichen complexen Zahlen, jede genau $2\lambda^2$ mal. Unter den conjugirten werden aber hier alle diejenigen verstanden, welche man erhält, indem man dem w seine λ Werthe $w, wa, \dots wa^{\lambda-1}$ giebt, und alsdann auch dem a (auch insofern es in $w = \sqrt[\lambda]{D(a)}$ enthalten ist) die Werthe $a, a^2 \dots a^{\lambda-1}$ giebt. Dabei wird die eine Hälfte der so entstandenen $\lambda(\lambda-1)$ Gleichungen der andern Hälfte gleich, und ist deshalb zu verwerfen, von den übrig bleibenden ν Gleichungen ist alsdann noch eine beliebige, als mit den übrigen identisch, wegzulassen, so daſs genau $\nu-1$ Gleichungen bleiben, mit ebenso vielen Gröſsen $y_1, y_2, \dots y_{\nu-1}$.

Mit Hülfe der Dirichletschen Sätze wird nun der Gränzwerth, welchen die Reihe R für $s=1$ annimmt, vollständig durch ein $\lambda(\lambda-1)$faches Integral bestimmt, nämlich:

$$(14.)\qquad R = \frac{C \cdot H}{2\lambda^2} \int dx_{0,0}\, dx_{0,1} \dots dx_{\lambda-2,\lambda-1},$$

in welchen die Gröſsen $x_{0,0}$ etc. als continuirliche Variable auftreten, und die Integrationen auf alle Werthe derselben von $-\infty$ bis $+\infty$ sich erstrecken, für welche die Variabeln $y_1, y_2 \dots y_{\nu-1}$ des obigen Systems in die Gränzen 0 und 1 zu liegen kommen, und für welche auch die Norm $NNF_0(w)$ in denselben Gränzen 0 und 1 liegt. Der Faktor C, welcher derselbe ist, als in der Gleichung (7.) rührt daher, daſs auch in $F_0(w)$ die Werthe ausgeschlossen sind, für welche $NF_0(w)$ durch ϱ, oder durch einen Primfaktor der Determinante $D(a)$ theilbar sein würde.

Dieses $\lambda(\lambda-1)$fache Integral wird nun zunächst so transformirt, daſs anstatt der Variabeln $x_{0,0}$ etc. die $\lambda(\lambda-1)$ zu $F_0(w)$ conjugirten complexen Zahlen, welche durch die zu der Gleichung (11.) conjugirten Gleichungen mit den alten Variabeln verbunden sind, als neue Variable eingeführt wer-

den. Die Funktional-Determinante dieser linearen Substitution erhält den einfachen Werth:

(15.) $$\delta = (-1)^{\frac{\mu}{2}} \lambda^{\frac{2\lambda^2 - 3\lambda}{2}} (ND(\alpha))^{\mu},$$

welcher nicht schwer zu finden ist.

Hierauf werden diese $\lambda(\lambda-1)$ Variabeln $F_0(w)$ mit allen conjugirten durch die Variabeln u_k und v_k ersetzt, welche aus jenen erhalten werden, indem man die Logarithmen derselben in die Form $u+\sqrt{-1}\,v$ setzt, wo u und v reale Gröfsen sind. Diese neue Substitution giebt:

(16.) $$R = \frac{2^{\nu} C \cdot H}{2\lambda^2 \delta} \int e^{2u_1} e^{2u_2} \dots e^{2u_\nu} du_1 du_2 \dots du_\nu dv_1 dv_2 \dots dv_\nu.$$

Da die Integrationen in Beziehung auf die Variabeln $v_1, v_2, \dots v_\nu$ alle in den Gränzen $-\frac{\pi}{2}$ bis $+\frac{3\pi}{2}$ auszuführen sind, so hat man hieraus das νfache Integral:

(17.) $$R = \frac{2^{2\nu} \pi^{\nu} C \cdot H}{2\lambda^2 \delta} \int e^{2u_1} e^{2u_2} \dots e^{2u_\nu} du_1 du_2 \dots du_\nu.$$

Wird die Integration in Beziehung auf u_ν in den, durch die Bedingung, dafs $NNF(w)$ positiv und kleiner als Eins sein mufs bestimmten Gränzen ausgeführt, so erhält man:

(18.) $$R = \frac{2^{2\nu} \pi^{\nu} C \cdot H}{4\lambda^2 \delta} \int du_1 du_2 \dots du_{\nu-1}.$$

Endlich werden nun anstatt dieser $\nu-1$ Variabeln die Variabeln $y_1, y_2 \dots y_{\nu-1}$ aus dem Systeme der Gleichungen, welche aus (13.) entstehen, eingeführt, und weil diese nur in den Gränzen 0 und 1 zu integriren sind, so erhält man:

(19.) $$R = \frac{2^{2\nu} \pi^{\nu} CH\Delta}{4\lambda^2 \delta}, \quad \text{für } s = 1,$$

wo Δ die Determinante aus den Logarithmen der analytischen Moduln der Fundamentaleinheiten in w und ihrer conjugirten bezeichnet.

Aus der Vergleichung dieses Resultats mit (9.) hat man nun den Ausdruck der Klassenzahl H, für die hier betrachtete Theorie der complexen Zahlen in w:

(20.) $$H = \frac{4\lambda^2 \delta K}{2^{2\nu} \pi^{\nu} \Delta C} \cdot L_1 L_2 L_3 \dots L_{\lambda-1},$$

oder wenn für K und δ ihre Werthe bei (8.) und (15.) gesetzt werden:

$$(21.) \qquad H = \frac{\lambda^{2\nu-3\mu+2}\,(ND(\alpha))^{\mu}\; P \cdot D}{2^{2\nu-\mu-1}\;\pi^{\nu-\mu}\;\Delta}\; L_1\, L_2\, L_3 \dots L_{\lambda-1}.$$

Die Summation der unendlichen Reihen L_1, L_2 ... würde diesem Ausdrucke erst seine Vollendung geben; dieselbe scheint aber äufserst schwierig zu sein, und bietet wenigstens den gewöhnlichen Mitteln Trotz. Für die Anwendung, die in dem Folgenden von dem gefundenen Resultate gemacht werden soll, kommt es aber nur darauf an, dafs das Produkt $L_1 L_2 \dots L_{\lambda-1}$, einen endlichen und von Null verschiedenen Werth hat, und dieses geht unmittelbar daraus hervor, dafs sowohl die Klassenanzahl H, als auch die Gröfsen Δ, P und D endliche, von Null verschiedene Werthe haben.

Die Klassenanzahl der complexen idealen Zahlen in z ist nur ein Vielfaches der gefundenen Klassenanzahl der idealen Zahlen in w, und zwar wird sie aus dieser durch Multiplikation mit einer Potenz von λ erhalten, deren nähere Bestimmung ich hier übergehe, weil sie für das Folgende nicht nöthig ist.

§. 7.

Eintheilung der verschiedenen Klassen der idealen Zahlen in z in ihre Gattungen.

Es soll nun die Theorie der complexen Zahlen in z in's Besondere, und zwar zunächst die Eintheilung der verschiedenen Klassen der idealen Zahlen dieser Theorie in ihre Gattungen (*Genera*) behandelt werden. Hierbei soll, wie überhaupt in allen folgenden Paragraphen dieser Abhandlung, angenommen werden, dafs die Primzahl λ nicht eine von denen ist, welche ich in meinen Untersuchungen über die complexen Zahlen in α als Ausnahmszahlen bezeichnet habe, also nicht eine solche, welche als Faktor des Zählers einer der ersten $\frac{\lambda-3}{2}$ Bernoullischen Zahlen vorkommt. Nach Ausschliessung dieser besonderen Werthe der Primzahl λ gelten für die complexen Zahlen und Einheiten dieser niederen Theorie folgende Sätze, welche ich in dem *Mémoire* in Liouville's Journal, Bd. 16, §. 9, und in der Abhandlung über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen in Crelle's Journal, Bd. 44, pag. 138 etc. bewiesen habe:

Die Klassenanzahl der idealen Zahlen in α ist nicht durch λ theilbar.

Der kleinste Exponent der Potenz, zu welcher eine ideale Zahl $f(\alpha)$ erhoben werden mufs, um zu einer wirklichen zu werden, ist nicht durch λ theilbar.

Jede Einheit $E(\alpha)$, welche einer nichtcomplexen ganzen Zahl congruent ist, nach dem Modul λ, ist eine λte Potenz einer anderen Einheit $\varepsilon(\alpha)$.

Jede nicht durch $1-\alpha$ theilbare, wirkliche complexe Zahl $F(\alpha)$ läfst sich durch Multiplikation mit einer passenden Einheit in die primäre Form bringen, in welcher sie die Bedingungen erfüllt: dafs erstens das Produkt $F(\alpha)\;F(\alpha^{-1})$ einer nichtcomplexen Zahl congruent ist, nach dem Modul λ, und dafs zweitens $F(\alpha)$ selbst einer nichtcomplexen Zahl congruent ist, nach dem Modul $(1-\alpha)^2$.

Es sei nun

$$F(z) = C + Bz + B_1 z_1 + \dots + B_{\lambda-1} z_{\lambda-1}$$

eine wirkliche complexe Zahl in z. Die Norm derselben, als Produkt aller conjugirten, ist eine symmetrische Funktion aller Wurzeln $z, z_1, \dots z_{\lambda-1}$ der Gleichung (5.), §. 1. In dieser Norm ist C^λ das einzige, kein z enthaltende Glied, aufser welchem noch symmetrische Funktionen der ersten, zweiten u. s. w. bis λten Dimension vorkommen. Alle diese symmetrischen Funktionen sind aber durch die Gleichungs-Coefficienten rational und ganz darstellbar, und müssen nothwendig alle den Faktor $\lambda\varrho$ enthalten, weil alle Gleichungscoefficienten denselben enthalten. Läfst man nun die durch $\lambda\varrho$ theilbaren Glieder der Norm weg, so hat man die Congruenz:

$$(1.) \qquad NF(z) \equiv C^\lambda, \text{ mod. } \lambda\varrho,$$

wo C eine ganze complexe Zahl in α ist. Bezeichnet man dieselbe durch $C(\alpha)$ und nimmt $NF(z) = F(\alpha)$, so hat man:

$$(2.) \qquad F(\alpha) \equiv C(\alpha)^\lambda, \text{ mod. } \lambda\varrho.$$

Weil die λte Potenz einer complexen Zahl in α einer nichtcomplexen Zahl congruent ist, nach dem Modul λ, so erkennt man hieraus, dafs die Norm jeder wirklichen complexen Zahl in z einer nichtcomplexen ganzen Zahl congruent ist, nach dem Modul λ.

Giebt man in der Congruenz (2.) dem α nach einander alle seine $\lambda-1$ Werthe, (wobei der Modul $\lambda\varrho$ wesentlich derselbe bleibt), und multiplicirt diese λ Congruenzen, so hat man:

$$NF(\alpha) \equiv (NC(\alpha))^\lambda, \text{ mod. } \lambda\varrho.$$

Weil nun $NC(\alpha)$, als Norm einer nicht durch ϱ theilbaren complexen Zahl in α, von der Form $1+m\lambda$ ist, die λte Potenz davon also von der Form $1+m\lambda^2$, weil ferner zwei nichtcomplexe ganze Zahlen, welche nach dem Modul $\lambda\varrho$ congruent sind, nothwendig auch nach dem Modul λ^2 congruent sein müssen, so hat man:

$$(3.)\qquad NF(\alpha) \equiv 1, \text{ mod. } \lambda^2.$$

Setzt man jetzt die wirkliche complexe Zahl $F(z)$ in die Form einer complexen Zahl in w:

$$F(z) = A + A_1 w + A_2 w^2 + \ldots + A_{\lambda-1} w^{\lambda-1},$$

und nimmt die Norm derselben, so ist diese Norm eine ganze rationale Funktion von w^λ, d. i. von $D(\alpha)$, und es ist A^λ das einzige Glied der Norm, welches w^λ nicht enthält. Läfst man nun alle Glieder weg, welche w^λ enthalten, so hat man die Congruenz:

$$(4.)\qquad NF(z) = F(\alpha) \equiv A^\lambda, \text{ mod. } D(\alpha).$$

Wenn nun die Determinante $D(\alpha)$ die von einander verschiedenen Primfaktoren $f(\alpha)$, $f_1(\alpha)$, $f_2(\alpha)$ ... enthält, welche ideal sein können, während $D(\alpha)$ als wirkliche complexe Zahl in α vorausgesetzt worden ist, so erkennt man aus dieser Congruenz, dafs in Beziehung auf alle diese Primfaktoren der Determinante die Norm der wirklichen complexen Zahl einer λten Potenz congruent ist, oder dafs man hat:

$$(5.)\qquad \left(\frac{F(\alpha)}{f(\alpha)}\right) = 1,\ \left(\frac{F(\alpha)}{f_1(\alpha)}\right) = 1,\ \left(\frac{F(\alpha)}{f_2(\alpha)}\right) = 1 \ldots\ldots$$

Aus den hier entwickelten Eigenschaften der Normen der wirklichen complexen Zahlen $F(z)$ ergeben sich nun die bestimmten Charaktere, welche die Normen der idealen Zahlen dieser Theorie besitzen. Die Norm einer idealen Zahl $F(z)$, als complexe Zahl in α, welche in dieser niederen Theorie auch selbst noch ideal sein kann, ist in Betreff der Einheiten in α, mit denen sie behaftet genommen werden kann, vollständig unbestimmt. Um diese Unbestimmtheit zu heben setze ich fest, dafs die Norm einer jeden idealen Zahl in z, als complexe Zahl in α, in der primären Form genommen werden soll, wie diese oben definirt ist, welche Bestimmung sich dadurch rechtfertigt, dafs sie für die Normen der wirklichen complexen Zahlen in z von selbst erfüllt ist, da jede solche Norm einer nicht complexen ganzen Zahl congruent ist, nach dem Modul λ, wie

oben gezeigt worden. Wenn $F(\alpha)$, als Norm der idealen Zahl $F(z)$, selbst noch ideal ist, so wird die niedrigste Potenz derselben, welche wirklich wird, in der primären Form genommen.

Wenn nun $F(z)$ eine ideale Zahl in z bezeichnet und $F(\alpha)$ die Norm derselben, wobei der Fall, daſs $F(z)$ auch wirklich sein kann, nicht ausgeschlossen wird, wenn ferner $f(\alpha)$, $f_1(\alpha)$ .... die verschiedenen, in der Determinante $D(\alpha)$ enthaltenen Primfaktoren sind und wenn die Determinante den Faktor $\varrho = 1 - \alpha$ nicht enthält, welche Bestimmung auch in dem Folgenden überall beibehalten werden soll: so sollen die Zahlenwerthe folgender $\frac{\lambda-3}{2}$ Differenzialquotienten des Logarithmus von $F(e^v)$:

$$(6.)\qquad \begin{aligned} \frac{d_0^3\, l\, F(e^v)}{dv^3} &\equiv C_3, \\ \frac{d_0^5\, l\, F(e^v)}{dv^5} &\equiv C_5, \qquad \text{mod. } \lambda, \\ &\;\vdots \\ \frac{d_0^{\lambda-2}\, l\, F(e^v)}{dv^{\lambda-2}} &\equiv C_{\lambda-2}, \end{aligned}$$

ferner die Zahl

$$(7.)\qquad \frac{1 - NF(\alpha)}{\lambda} \equiv C_{\lambda-1}, \text{ mod. } \lambda.$$

und endlich auch die, durch die Legendreschen Zeichen:

$$(8.)\qquad \begin{aligned} \left(\frac{F(\alpha)}{f(\alpha)}\right) &= \alpha^{K} \\ \left(\frac{F(\alpha)}{f_1(\alpha)}\right) &= \alpha^{K_1} \end{aligned}$$

u. s. w. bestimmten Zahlen K, K_1 .... als Charaktere der idealen Zahl $F(z)$, oder auch als Charaktere der Norm derselben $F(\alpha)$ bezeichnet werden. Aus dieser Erklärung der Charaktere ergiebt sich zunächst fast unmittelbar der Satz:

(I.) Die Charaktere des Produkts zweier oder mehrerer idealen Zahlen werden gefunden, wenn man die Charaktere der einzelnen Faktoren zu einander addirt.

Für die, als Differenzialquotienten der Logarithmen ausgedrückten Charaktere folgt die Richtigkeit dieses Satzes aus der analogen Eigenschaft der Logarithmen, und für die durch die Legendreschen Zeichen definirten aus der Eigenschaft dieser Zeichen, nach welcher

$$\left(\frac{F(\alpha)\cdot\phi(\alpha)}{f(\alpha)}\right) = \left(\frac{F(\alpha)}{f(\alpha)}\right)\left(\frac{\phi(\alpha)}{f(\alpha)}\right)$$

ist. Um dieselbe auch für den mit $C_{\lambda-1}$ bezeichneten Charakter nachzuweisen, kann man von der Congruenz

$$(1 - NF(\alpha))\,(1 - N\phi(\alpha)) \equiv 0, \text{ mod. } \lambda^2,$$

ausgehen, welche nothwendig Statt hat, weil sowohl $1 - NF(\alpha)$ als $1 - N\phi(\alpha)$ durch λ theilbar sind. Entwickelt man das Produkt dieser beiden Faktoren, bringt $NF(\alpha)\ N\phi(\alpha)$ auf die andere Seite, addirt auf beiden Seiten Eins und dividirt durch λ, so hat man:

$$\text{(9.)}\qquad \frac{1 - NF(\alpha)}{\lambda} + \frac{1 - N\phi(\alpha)}{\lambda} \equiv \frac{1 - N(F(\alpha)\phi(\alpha))}{\lambda}, \text{ mod. } \lambda,$$

und der auf diese Weise für zwei Faktoren geführte Beweis wird durch bloſse Wiederholung auf beliebig viele Faktoren ausgedehnt, und giebt, wenn die Faktoren einander gleich angenommen werden:

$$\text{(10.)}\qquad \frac{k\,(1 - NF(\alpha))}{\lambda} \equiv \frac{1 - NF(\alpha)^k}{\lambda}, \text{ mod. } \lambda.$$

Die Benennung Charaktere kommt diesen Zahlen darum zu, weil sie nicht nur einzelnen idealen Zahlen angehören, sondern für alle idealen Zahlen einer Klasse dieselben bleiben. Um dieſs zu beweisen, bemerke ich zunächst, daſs für die Klasse der wirklichen complexen Zahlen in z alle diese Charaktere den Werth Null haben. In der That sind erstens die $\frac{\lambda-3}{2}$, als Differenzialquotienten von $lF(e^v)$ definirten, alle congruent Null, weil $F(\alpha)$ einer λten Potenz congruent ist, nach dem Modul λ; zweitens ist der Charakter $C_{\lambda-1}$ congruent Null, weil $1 - NF(\alpha)$ durch λ^2 theilbar ist, und drittens sind auch K, K_1, ... congruent Null, weil $F(\alpha)$ einer λten Potenz congruent ist, nach dem Modul $D(\alpha)$, und somit auch nach den Moduln $f(\alpha)$, $f_1(\alpha)$ .... Es seien nun $F_r(z)$ und $F_s(z)$ zwei äquivalente ideale Zahlen, und $\Phi(z)$ ein Multiplikator, welcher beide zu wirklichen macht, also sowohl $\Phi(z)\ F_r(z)$ als auch $\Phi(z)\ F_s(z)$ wirklich. Es sei auch $NF_r(z) \doteq F_r(\alpha)$, $NF_s(z) \doteq F_s(\alpha)$ und $N\Phi(z) \doteq \Phi(\alpha)$, so hat man:

$$\frac{d_0^{2n+1}\, l\left(\Phi(e^v)\cdot F_r(e^v)\right)}{dv^{2n+1}} \equiv 0, \text{ mod. } \lambda,$$

$$\frac{d_0^{2n+1}\, l\left(\Phi(e^v)\cdot F_s(e^v)\right)}{dv^{2n+1}} \equiv 0, \text{ mod. } \lambda,$$

also auch

(11.) $$\frac{d^{2n+1}\, l F_r(e^v)}{dv^{2n+1}} \equiv \frac{d^{2n+1}\, l F_s(e^v)}{dv^{2n+1}}, \text{ mod. } \lambda.$$

Ferner hat man für die Normen der **wirklichen** Zahlen $\Phi(z)\, F_r(z)$ und $\Phi(z)\, F_s(z)$:

$$N(\Phi(\alpha)\, F_r(\alpha)) \equiv 1, \text{ mod. } \lambda^2,$$
$$N(\Phi(\alpha)\, F_s(\alpha)) \equiv 1, \text{ mod. } \lambda^2,$$

woraus folgt:

$$NF_r(\alpha) \equiv NF_s(\alpha), \text{ mod. } \lambda^2,$$

und

(12.) $$\frac{NF_r(\alpha)-1}{\lambda} \equiv \frac{NF_s(\alpha)-1}{\lambda}, \text{ mod. } \lambda.$$

Endlich hat man auch für die Normen dieser **wirklichen** Zahlen:

$$\left(\frac{\Phi(\alpha)\, F_r(\alpha)}{f(\alpha)}\right) = 1, \ \left(\frac{\Phi(\alpha)\, F_s(\alpha)}{f(\alpha)}\right) = 1,$$

also

$$\left(\frac{\Phi(\alpha)}{f(\alpha)}\right) \cdot \left(\frac{F_r(\alpha)}{f(\alpha)}\right) = 1, \ \left(\frac{\Phi(\alpha)}{f(\alpha)}\right) \cdot \left(\frac{F_s(\alpha)}{f(\alpha)}\right) = 1,$$

demnach

(13.) $$\left(\frac{F_r(\alpha)}{f(\alpha)}\right) = \left(\frac{F_s(\alpha)}{f(\alpha)}\right),$$

und ebenso für alle verschiedenen Primfaktoren $f_1(\alpha)$, $f_2(\alpha)$ ... der Determinante. Man hat also den Satz:

(II.) **Alle äquivalenten, einer und derselben Klasse angehörenden, idealen Zahlen haben gleiche Charaktere.**

Die aufgestellten Charaktere sind somit nicht blofs Charaktere der einzelnen idealen Zahlen, sondern Charaktere der Klassen. Aus diesem Grunde wird auf sie die Eintheilung der Klassen in die Gattungen (*Genera*) gegründet, indem alle nicht äquivalenten Klassen, welche vollständig dieselben Charaktere haben, einer und derselben Gattung, diejenigen aber, für welche nicht alle Charaktere dieselben sind, verschiedenen Gattungen zugetheilt werden.

Wenn die Anzahl der verschiedenen, in der Determinante $D(\alpha)$ enthaltenen Primfaktoren gleich r ist, so giebt es für jede ideale Zahl in z $\frac{\lambda-1}{2}+r$ besondere Charaktere, deren jeder einen der λ Werthe 0, 1, 2, ...

$\lambda - 1$ haben kann. Die Anzahl aller möglichen Combinationen dieser Werthe der einzelnen Charaktere ist gleich der $(\frac{\lambda-1}{2} + r)$ten Potenz von λ, welches also die Anzahl aller Gesammtcharaktere ist die überhaupt möglicherweise Statt haben können, oder die Anzahl aller angebbaren Gattungen. Weil aber der Fall eintreten kann, und wie in dem Folgenden gezeigt werden wird auch wirklich eintritt, dafs gewisse dieser angebbaren Gattungen gar keine Klassen idealer Zahlen enthalten, so sind von diesen blofs angebbaren, die wirklich vorhandenen Gattungen wohl zu unterscheiden. Diejenige Gattung, deren Charaktere alle gleich Null sind, welcher, wie oben gezeigt worden ist die Klasse der wirklichen complexen Zahlen angehört, welche also immer eine wirklich vorhandene ist, soll die Hauptgattung (*Genus principale*) genannt werden.

Über die Vertheilung der einzelnen Klassen in die Gattungen wird nun zunächst folgender Satz bewiesen:

(III.) Alle wirklich vorhandenen Gattungen enthalten gleich viele Klassen idealer Zahlen.

Setzt man nämlich alle Klassen einer gegebenen Gattung mit einer bestimmten Klasse zusammen, so gehören alle dadurch entstehenden verschiedenen Klassen wieder einer und derselben Gattung an, weil sie, wie der Satz (I.) zeigt, alle dieselben Charaktere haben. Durch passende Wahl dieser einen Klasse kann man aber aus einer jeden gegebenen Gattung, welche n Klassen enthält eben so viele verschiedene Klassen einer jeden anderen gegebenen Gattung erzeugen. Wählt man nun für die eine Gattung, aus welcher alle übrigen erzeugt werden, eine solche, welche nicht weniger Klassen enthält als irgend eine andere, so folgt, dafs alle anderen Klassen nicht nur nicht mehr, sondern auch nicht weniger Klassen enthalten können als diese, wodurch die Richtigkeit des Satzes bewiesen ist.

Aufser der Eintheilung in die Gattungen ist noch eine andere Eintheilung der nichtäquivalenten Klassen beachtenswerth, welche von den verschiedenen Klassen der idealen Zahlen in α herrührt. Wenn h die Anzahl der nichtäquivalenten Klassen dieser niederen Theorie ist, und die idealen Zahlen $\phi(\alpha)$, $\phi_1(\alpha)$, $\phi_2(\alpha)$, ... $\phi_{h-1}(\alpha)$ repräsentiren diese verschiedenen Klassen, wenn ferner $F(z)$ eine ideale Zahl in z ist, so stellen

$$\phi(\alpha)F(z), \quad \phi_1(\alpha)F(z), \quad .... \quad \phi_{h-1}(\alpha)F(z)$$

h nichtäquivalente Klassen dieser höheren Theorie dar, welche in gewissem Sinne als zusammengehörig zu betrachten sind, und eine Gruppe bilden. Ist $F_1(z)$ eine nicht in dieser Gruppe enthaltene ideale Zahl, so hat man aus ihr eine zweite Gruppe von Klassen:

$$\phi(\alpha)F_1(z),\ \ \phi_1(\alpha)F_1(z),\ \ \ldots.\ \ \phi_{h-1}(\alpha)F_1(z)\ ,$$

welche weder unter sich, noch mit den Klassen der ersten Gruppe äquivalent sind. In dieser Weise fortfahrend kann man alle Klassen der idealen Zahlen in z in solche Gruppen von je h Klassen zusammenfassen, woraus beiläufig folgt, dafs die Klassenanzahl der idealen Zahlen in z durch die Klassenanzahl der idealen Zahlen in α theilbar ist. Diese Eintheilung in die Gruppen wird bei einigen der zu erörternden Hauptfragen ihre Anwendung finden, in welchen der Unterschied der, einer und derselben Gruppe angehörenden Klassen nur als ein unwesentlicher anzusehen sein wird. Aus diesem Grunde sollen nur diejenigen Klassen der idealen Zahlen in z, welche verschiedenen Gruppen angehören, wesentlich verschiedene Klassen benannt werden. Nimmt man aus jeder Klasse eine einzige ideale Zahl, welche als Repräsentant der ganzen Klasse angesehen wird, so kann man dieselbe immer so wählen, dafs sie keinen wirklichen Faktor enthält, namentlich auch keinen wirklichen Faktor, welcher nur eine complexe Zahl in α ist, weil durch das Weglassen eines wirklichen Faktors an der Klasse, welcher eine ideale Zahl angehört, nichts geändert wird. Nimmt man ferner aus jeder der Gruppen von h Klassen eine der idealen Zahlen, welche diese Klassen repräsentiren, als Repräsentant der Gruppe, so kann man dieselbe immer so wählen, dafs sie niemals alle λ conjugirten idealen Primfaktoren irgend einer idealen Primzahl $\phi(\alpha)$ der niederen Theorie, und somit $\phi(\alpha)$ selbst als Faktor enthält; denn wenn man den idealen Faktor $\phi(\alpha)$ aus der idealen Zahl wegläfst, so erhält man eine ideale Zahl derselben Gruppe. Schliefst man, wie es bei gewissen Untersuchungen nützlich ist, diejenigen idealen Zahlen in z vollständig aus, welche ideale Faktoren $\phi(\alpha)$ der niederen Theorie enthalten, so gehören alle nichtäquivalenten Klassen nothwendig auch verschiedenen Gruppen an, und geben darum nur alle diejenigen Klassen, welche wir als wesentlich verschiedene bezeichnet haben. Die Anzahl dieser ist gleich dem $h$ten Theile der Anzahl aller nichtäquivalenten Klassen.

Die Eintheilung in die Gruppen ordnet sich der Eintheilung in die Gattungen vollständig unter, da alle Klassen einer und derselben Gruppe nothwendig auch einer und derselben Gattung angehören. Die Charaktere der idealen Zahlen $\phi(\alpha)$, $\phi_1(\alpha)$, ... $\phi_{h-1}(\alpha)$, welche hier als ideale Zahlen in z auftreten, sind nämlich alle gleich Null, weil die Normen dieser idealen Zahlen in Beziehung auf z nur die λten Potenzen derselben sind, ihre Charaktere also alle gleich Null, so dafs durch das Hinzutreten derselben an den Charakteren einer idealen Zahl $F(z)$ nichts geändert wird.

Conjugirte ideale Zahlen gehören im Allgemeinen verschiedenen Klassen und verschiedenen Gruppen, aber stets nur einer und derselben Gattung an, weil die Charaktere nur von der Norm abhängen, welche für alle conjugirten dieselbe ist. Wenn aber von conjugirten Zahlen zwei derselben Klasse angehören, also äquivalent sind, so sind alle λ conjugirten äquivalent; denn wenn $\phi(z)$ eine ideale Zahl ist, welche einer ihrer conjugirten $\phi(z_k)$ äquivalent ist, so giebt es einen Multiplikator $\psi(z)$, für welchen $\psi(z)\,\phi(z)$ und $\psi(z)\,\phi(z_k)$ beide zugleich wirklich sind; verwandelt man nun z in z_k, so sind auch $\psi(z_k)\,\phi(z_k)$ und $\psi(z_k)\,\phi(z_{2k})$ beide zugleich wirklich, woraus $\phi(z_k)$ äquivalent mit $\phi(z_{2k})$ geschlossen wird, und auf diese Weise weiter fortschliefsend sieht man, dafs alle conjugirten äquivalent sind.

Eine ideale Zahl, welche die Eigenschaft hat, dafs sie ihren conjugirten äquivalent ist, soll eine **ambige ideale Zahl** genannt werden, und die Klasse, welcher sie angehört, eine **ambige Klasse**, ähnlich wie bei **Gaufs** in der Theorie der quadratischen Formen, diejenige Klasse, welche eine ihrer entgegengesetzten, also conjugirten äquivalente Form enthält, als *Classis anceps* bezeichnet wird. In Betreff der Gruppen von je h Gliedern ist zu bemerken, dafs wenn eine Klasse einer Gruppe eine ambige ist, nothwendig alle h Klassen derselben ambige sein müssen.

Die Anzahl der ambigen Klassen, und namentlich der wesentlich verschiedenen, steht mit der Anzahl der wirklich vorhandenen Gattungen in einem sehr innigen Zusammenhange, welcher in dem Folgenden genauer erörtert werden wird. Für jetzt soll in dieser Beziehung nur der eine Hauptsatz bewiesen werden:

(IV.) **Die Anzahl aller wirklich vorhandenen Gattungen ist nicht gröfser, als die Anzahl aller wesentlich verschiedenen, nicht äquivalenten ambigen Klassen.**

Wenn $f(z)$ eine beliebige ideale Zahl ist, $f(z_1)$ ihre erste conjugirte, so giebt es immer eine ideale Zahl $F(z)$ von der Art, dafs $F(z)f(z_1)$ mit $f(z)$ äquivalent ist, welches ich so ausdrücke:

(14.) $$f(z) \text{ aeqv. } F(z)f(z_1).$$

Untersucht man nun, unter welcher Bedingung zwei verschiedene Klassen idealer Zahlen, welche durch $f(z)$ und $g(z)$ repräsentirt werden, in dieser Äquivalenz eine und dieselbe Klasse $F(z)$ ergeben, indem man diese Äquivalenz mit der folgenden:

$$g(z) \text{ aeqv. } F(z)\,g(z_1)$$

verbindet, so kann man die Klasse $g(z)$ durch $f(z)\,\phi(z)$ ersetzen, wo $\phi(z)$ stets so bestimmt werden kann, dafs $g(z)$ äquivalent $f(z)\,\phi(z)$ ist, woraus sodann geschlossen wird, dafs auch die conjugirte Zahl $g(z_1)$ der conjugirten $f(z_1)\,\phi(z_1)$ äquivalent ist. Man hat daher:

$$f(z)\,\phi(z) \text{ aeqv. } F(z)\,f(z_1)\,\phi(z_1)$$

und hieraus nach der Äquivalenz (14.):

$$\phi(z) \text{ aeqv. } \phi(z_1),$$

woraus folgt, dafs $\phi(z)$ eine Ambige sein mufs, und umgekehrt, wenn $\phi(z)$ eine Ambige ist, dafs $f(z)$ und $f(z)\,\phi(z)$ in der Äquivalenz (14.) dieselbe Klasse $F(z)$ ergeben. Also alle diejenigen verschiedenen Klassen $f(z)$, welche aus einer derselben entstehen, indem man dieselbe mit allen ambigen Klassen zusammensetzt, ergeben für $F(z)$ eine und dieselbe Klasse, diejenigen aber, welche nicht auf diese Weise aus einer einzigen erzeugt werden können, ergeben verschiedene Klassen für $F(z)$. Wenn man nun bei dieser Frage nur wesentlich verschiedene Klassen in Betracht zieht, und die Anzahl derselben mit $\mathfrak{H}$, die Anzahl der wesentlich verschiedenen Klassen aber mit $\mathfrak{A}$ bezeichnet, so hat man die Anzahl aller wesentlich verschiedenen Klassen $F(z)$, welche der Äquivalenz (14.) genügen, wenn für $f(z)$ alle verschiedenen Klassen genommen werden, gleich $\frac{\mathfrak{H}}{\mathfrak{A}}$.

Es gehört nun aber jede Klasse $F(z)$, welche der Äquivalenz (14.) genügen kann, nothwendig der Hauptgattung an, deren Charaktere alle gleich Null sind; denn die Charaktere des Produkts $F(z)f(z_1)$ findet man, indem man die Charaktere von $F(z)$ zu den entsprechenden von $f(z_1)$, die

denen von $f(z)$ gleich sind, addirt, und weil die Charaktere von $F(z)f(z_1)$ denen von $f(z)$, wegen der Äquivalenz beider idealen Zahlen, gleich sind, so folgt, dafs die Charaktere von $F(z)$ alle gleich Null sein müssen.

Die Hauptgattung enthält also nothwendig diese $\frac{\mathfrak{H}}{\mathfrak{A}}$ wesentlich verschiedenen Klassen, wobei der Fall nicht ausgeschlossen ist, dafs sie aufserdem auch noch andere enthalten könnte. Da aber alle wirklich vorhandenen Gattungen gleich viele Klassen, und darum auch gleich viele der wesentlich verschiedenen Klassen enthalten, so folgt, dafs jede der vorhandenen Gattungen mindestens $\frac{\mathfrak{H}}{\mathfrak{A}}$ wesentlich verschiedene Klassen enthält, wodurch der aufgestellte Satz bewiesen ist.

§. 8.

Die idealen ambigen Zahlen, insofern sie in gewissen wirklichen complexen Zahlen in z enthalten sind.

Sei $\phi(z)$ eine ideale Ambige, und zwar eine solche, welche nicht alle λ conjugirten idealen Primfaktoren einer Primzahl $\phi(\alpha)$ der niederen Theorie und keinen complexen Primfaktor in α welcher in der Theorie der complexen Zahlen in z Primfaktor ist, also überhaupt keinen idealen oder wirklichen Faktor dieser niederen Theorie enthält. Sei ferner $\psi(z)$ ein idealer Multiplikator, welcher mit $\phi(z)$ und der conjugirten $\phi(z_1)$ zusammengesetzt, wirkliche complexe Zahlen ergiebt, so dafs

$$G(z) = \psi(z)\,\phi(z) \text{ und } G_1(z) = \psi(z)\,\phi(z_1)$$

wirkliche complexe Zahlen sind. Da $G(z)$ und $G(z_1)$, lediglich durch die idealen Faktoren bestimmt sind, welche sie enthalten, so können sie beliebig mit Einheiten in z behaftet angenommen werden, diese können aber stets so gewählt werden, dafs die Normen der Zahlen $G(z)$ und $G_1(z)$ einander gleich werden. Die Normen $NG(z)$ und $NG_1(z)$ sind nämlich erstens genau aus denselben idealen Faktoren in z zusammengesetzt, und können sich daher nur durch eine Einheit in z unterscheiden, sie sind zweitens complexe Zahlen der niederen Theorie in α, darum kann diese Einheit, durch welche sie sich unterscheiden, nur eine Einheit $E(\alpha)$ sein, und man hat

$$NG(z) = E(\alpha)\, NG_1(z).$$

Die Normen aller **wirklichen** complexen Zahlen in z sind aber, nach dem Modul λ, nichtcomplexen ganzen Zahlen congruent, es mufs also auch die Einheit $E(\alpha)$ einer nichtcomplexen Zahl congruent sein, nach dem Modul λ, also in Folge des im §. 7. citirten Satzes, mufs sie eine λte Potenz einer Einheit sein, also:

$$E(\alpha) = \varepsilon(\alpha)^\lambda.$$

Nimmt man $\varepsilon(\alpha)\, G(z)$ anstatt $G(z)$, wozu man berechtigt ist, weil die Wahl der $G(z)$ und $G_1(z)$ behaftenden Einheiten völlig frei ist, so hat man:

$$NG(z) = NG_1(z). \tag{1.}$$

Wenn nun $G(z)$ und $G_1(z)$ so gewählt sind, dafs sie dieser Bedingung genügen, so setze ich

$$\frac{G(z)}{G_1(z)} = E(z). \tag{2.}$$

Aus dieser gebrochenen complexen Zahl $E(z)$, deren Norm gleich Eins ist, bilde ich einen der Ausdrücke, deren Theorie ich in **Crelle's** Journal, Bd. 50, pag. 212 behandelt habe, nämlich

$$\begin{aligned} P(E(z)) = 1 + E(z) + E(z)E(z_1) + E(z)E(z_1)E(z_2) + \ldots \\ \ldots + E(z)E(z_1)\ldots E(z_{\lambda-2}). \end{aligned} \tag{3.}$$

Dieser Ausdruck, welcher selbst eine wirkliche gebrochene complexe Zahl in z ist, kann, wenn die Wurzeln z, aus den Nennern der Brüche entfernt werden, in folgende Form gesetzt werden:

$$PE(z) = \frac{Af(z)}{B}, \tag{4.}$$

wo A und B wirkliche complexe Zahlen in α sind, und $f(z)$ eine wirkliche ganze complexe Zahl in z. Vermöge der ersten allgemeinen Grundeigenschaft des mit $PE(z)$ bezeichneten Ausdrucks, nämlich

$$E(z)\, P(E(z_1)) = P(E(z)),$$

hat man nun, wenn man die Form (4.) einsetzt, und $\frac{A}{B}$ als gemeinschaftlichen Faktor wegläfst:

$$E(z) f(z_1) = f(z),$$

oder, wenn für $E(z)$ sein Werth bei (2.) zurückgesetzt, und mit $G_1(z)$ multiplicirt wird:

$$G(z)f(z_1) = G_1(z)f(z). \tag{5.}$$

Es ist hier zu bemerken, dafs der weggehobene gemeinschaftliche Faktor $\frac{A}{B}$ unter Umständen gleich Null sein kann, und dafs dadurch diese Gleichungen illusorisch werden können, nämlich wenn $PE(z)$ gleich Null ist. In diesem Falle kann man aber anstatt der Einheit $E(z)$ die Einheit $\alpha^k E(z)$ nehmen und die Zahl k so bestimmen, dafs $P(\alpha^k E(z))$ nicht gleich Null ist. Dafs unter den λ Werthen dieses Ausdrucks für $k = 0, 1, 2, \ldots \lambda - 1$, wenigstens einer nicht gleich Null ist, folgt unmittelbar daraus, dafs die Summe derselben gleich λ ist. Dieselbe Bemerkung ist ebenso auf alle Anwendungen zu beziehen, welche in dem Folgenden von diesen aus Einheiten zusammengesetzten Ausdrücken gemacht werden mögen.

Die ideale Ambige $\phi(z)$ hat die Eigenschaft, dafs ihre $h\lambda$te Potenz wirklich ist, wenn h die Klassenanzahl der idealen complexen Zahlen in α bezeichnet; denn weil die Ambige allen ihren conjugirten äquivalent ist, so hat man:

$$N\phi(z) \text{ aeqv. } \phi(z)^\lambda$$

und wenn zur $h$ten Potenz erhoben wird, so wird $(NF(z))^h$ wirklich, weil $N\phi(z)$ nur eine complexe ideale Zahl in α ist, deren $h$te Potenz nothwendig wirklich ist; es ist also auch $\phi(z)^{h\lambda}$ wirklich. Setzt man nun

$$\phi(z)^{h\lambda} = \Phi(z), \quad \psi(z)^{h\lambda} = \Psi(z),$$

wo $\Phi(z)$ und $\Psi(z)$ wirklich sind, so hat man:

$$\begin{aligned} G(z)^{h\lambda} &= \Psi(z)\, \Phi(z)\, \varepsilon(z) \\ G_1(z)^{h\lambda} &= \Psi(z)\, \Phi(z_1)\, \varepsilon_1(z) \end{aligned}$$

und darum giebt die Gleichung (5.) zur $h\lambda$ten Potenz erhoben, wenn der gemeinschaftliche wirkliche Faktor $\Psi(z)$ hinweggehoben, und der Quotient der beiden Einheiten $\varepsilon(z)$ und $\varepsilon_1(z)$ durch $e(z)$ bezeichnet wird:

$$e(z)\, \Phi(z) f(z_1)^{h\lambda} = \Phi(z_1) f(z)^{h\lambda}. \tag{6.}$$

Die Einheit $e(z)$ ist hier eine ganze Einheit, und zwar eine solche, deren Norm gleich Eins ist. Man hat nun:

$$(7.)\qquad \frac{f(z)^{h\lambda}}{\Phi(z)} = \frac{f(z)^{h\lambda}\,\Phi(z_1)\,\Phi(z_2)\,\ldots\,\Phi(z_{\lambda-1})}{N\Phi(z)} = \frac{F(z)}{N\Phi(z)},$$

wenn dieser Zähler der Einfachheit wegen durch $F(z)$ bezeichnet wird, und demnach aus der Gleichung (6.):

$$(8.)\qquad e(z)\,F(z_1) = F(z).$$

Die complexe Zahl $F(z)$, welche dieser Gleichung (8.) genügt, hat die Eigenschaft, dafs sie zu jedem idealen Primfaktor, welchen sie enthält, auch alle seine conjugirten enthalten mufs. Ist nämlich $p(z)$ ein in $F(z)$ enthaltener idealer Primfaktor, so mufs vermöge der Gleichung (8.) derselbe auch in $F(z_1)$ enthalten sein, und wenn z in $z_{\lambda-1}$, z_1 in z, u. s. w. verwandelt wird, wodurch $F(z_1)$ in $F(z)$ übergeht, so folgt, dafs $F(z)$ auch den Primfaktor $p(z_{\lambda-1})$ enthalten mufs. Hieraus folgt weiter, vermöge der Gleichung (8.), dafs auch $F(z_1)$ den Primfaktor $p(z_{\lambda-1})$ enthalten mufs, und wenn wieder z in $z_{\lambda-1}$ verwandelt wird, dafs $F(z)$ den Faktor $p(z_{\lambda-2})$ enthalten mufs. So fortschliefsend findet man, dafs $F(z)$ alle λ conjugirten idealen Primfaktoren, und folglich die complexe Primzahl $p(\alpha)$ der niederen Theorie enthalten mufs, zu welcher sich dieselben zusammensetzen. Da dasselbe für alle definirten idealen Primfaktoren gilt, so folgt, dafs $F(z)$ sich in zwei Faktoren zerlegen läfst, deren einer nur eine complexe Zahl in α ist, der andere aber eine complexe Zahl in z, welche die Eigenschaft hat, keinen der definirten idealen Primfaktoren zu enthalten. Der erste dieser Faktoren könnte auch eine ideale Zahl in α sein, um ihn also gewifs zu einem wirklichen zu machen, erhebe ich $F(z)$ zur $h$ten Potenz, weil hierdurch, wenn h die Klassenanzahl der idealen Zahlen in α ist, der erste Faktor wirklich wird, so mufs der zweite auch wirklich werden, und es wird:

$$(9.)\qquad F(z)^h = C\Delta(z),$$

wo C eine wirkliche complexe Zahl in α ist, und $\Delta(z)$ eine wirkliche complexe Zahl in z, welche keinen der definirten idealen Primfaktoren enthält, deren Norm also lediglich aus den Faktoren der Determinante $D(\alpha)$ und einer Potenz von ϱ bestehen kann.

Ich erhebe nun die Gleichung (7.) zur $h$ten Potenz, und setze den gefundenen Werth des $F(z)^h$ ein, so wird:

$$(10.)\qquad f(z)^{h^2\lambda} = \frac{C\Delta(z)\,\Phi(z)^h}{(N\Phi(z))^h}.$$

Es sei nun $p(z)$ ein idealer Primfaktor von $\phi(z)$, also auch von $\Phi(z)$, so enthält $N\Phi(z)$ alle seine conjugirten, welche zusammen den Primfaktor $p(\alpha)$ der niederen Theorie bilden. $\Phi(z)^k$ im Zähler, enthält (nach der Voraussetzung, daſs $\phi(z)$ nicht einen idealen Faktor in α enthalten soll,) nicht alle conjugirten idealen Primfaktoren zu $p(z)$, $\Delta(z)$ enthält keinen derselben, also muſs C einen oder einige derselben enthalten, weil alle diese Faktoren des Nenners gegen die des Zählers sich hinwegheben müssen. C aber, als complexe Zahl in α, kann nicht ideale Primfaktoren in z enthalten, ohne daſs sie alle conjugirten zugleich, und folglich $p(\alpha)$ enthält. Der Faktor $p(\alpha)$ des Nenners $(N\Phi(z))^k$ hebt sich also vollständig gegen den Faktor C des Zählers hinweg, und weil dasselbe für alle Faktoren des Nenners gilt, so folgt, daſs C durch $(N\Phi(z))^k$ theilbar ist. Bezeichnet man diesen Quotienten mit K, so hat man:

$$f(z)^{h^2\lambda} = K\Delta(z)\,\Phi(z)^k \tag{11.}$$

und wenn durch $\phi(z)^{h^2\lambda} = \Phi(z)^k$ dividirt wird:

$$\left(\frac{f(z)}{\phi(z)}\right)^{h^2\lambda} = K\Delta(z). \tag{12.}$$

Hieraus folgt, daſs $f(z)$ alle idealen Primfaktoren des $\phi(z)$ enthalten muſs, und ferner, daſs zu jedem idealen Primfaktor in z, welchen es ausserdem enthalten könnte, alle conjugirten in $f(z)$ enthalten sein müssen, welche sich zu einer complexen Zahl in α zusammensetzen. Verbindet man diese complexe Zahl in α mit der Ambigen $\phi(z)$, wodurch dieselbe in eine andere, derselben Gruppe angehörende, also nicht wesentlich verschiedene Ambige übergeht, so läſst sich das gefundene Resultat so aussprechen:

(I.) Jede ideale Ambige $\phi(z)$, wenn sie von den Faktoren, welche sich zu idealen oder wirklichen complexen Zahlen in α zusammensetzen, befreit angenommen wird, ist in einer wirklichen complexen Zahl $f(z)$ so enthalten, daſs diese wirkliche Zahl $f(z)$ die ideale Ambige $\phi(z)$, aber ausserdem keinen der definirten idealen Primfaktoren weiter enthält.

Wenn alle in einer wirklichen complexen Zahl $f(z)$ enthaltenen, idealen Primfaktoren zusammen eine Ambige $\phi(z)$ ausmachen, so soll von der Zahl $f(z)$ ausgesagt werden: sie enthält die Ambige $\phi(z)$.

Wenn nun $f(z)$ die Ambige $\phi(z)$ enthält, so ist

$$(13.)\qquad Nf(z) = \Delta(\alpha)\cdot N\phi(z),$$

und es enthält $\Delta(\alpha)$ keine anderen Primfaktoren in α, als die in der Determinante $D(\alpha)$ enthaltenen, und ausserdem eine Potenz von ϱ.

Es sollen nun die nothwendigen und hinreichenden Bedingungen dafür gefunden werden, dafs eine wirkliche complexe Zahl in z eine ideale Ambige enthalte. Es sei also $\phi(z)$ eine ideale Ambige, welche in der wirklichen Zahl $f(z)$ enthalten ist, so ist der Complex aller in $f(z)^{h^{\lambda-1}} f(z_1)$ enthaltenen idealen Faktoren gleich $\phi(z)^{h^{\lambda-1}} \phi(z_1)$, welches, wegen der Bedingung $\phi(z)$ aeqv. $\phi(z_1)$, mit $\phi(z)^{h^{\lambda}}$, also mit einer wirklichen complexen Zahl äquivalent, und darum selbst wirklich ist. Setzt man nun der Kürze wegen:

$$(14.)\qquad \phi(z)^{h^{\lambda-1}} \phi(z_1) = \Phi(z),$$

so hat man:

$$(15.)\qquad f(z)^{h^{\lambda-1}} f(z_1) = \Delta(z)\,\Phi(z),$$

wo $\Delta(z)$ und $\Phi(z)$ zwei wirkliche complexe Zahlen sind, deren erste keinen idealen Primfaktor in z enthält, und darum in ihrer Norm nur die in $\varrho D(\alpha)$ enthaltenen Primfaktoren haben kann, von denen dagegen die zweite nur aus idealen Primfaktoren in z zusammengesetzt, also ihre Norm zu $\varrho D(\alpha)$ relative Primzahl ist. Umgekehrt, wenn der Complex aller in $f(z)^{h^{\lambda-1}} f(z_1)$ enthaltenen idealen Primfaktoren eine wirkliche complexe Zahl in z ist, und $\phi(z)$ stellt den Complex aller in $f(z)$ enthaltenen idealen Primfaktoren dar, so ist $\phi(z)^{h^{\lambda-1}} \phi(z_1)$ wirklich, und hieraus folgt, dafs $\phi(z)$ äquivalent $\phi(z_1)$, also eine Ambige ist. Man hat daher folgenden Satz:

(II.) **Wenn die wirkliche complexe Zahl $\phi(z)$ eine Ambige enthält, so läfst sich $f(z)^{h^{\lambda-1}} f(z_1)$ in zwei wirkliche Faktoren zerlegen, welche so beschaffen sind, dafs die Norm des einen nur die Primfaktoren von $\varrho D(\alpha)$, die Norm des andern dagegen keinen dieser Primfaktoren enthält, und umgekehrt: wenn diese complexe Zahl eine solche Zerlegung in zwei Faktoren gestattet, so enthält $f(z)$ eine Ambige.**

Man kann die Bedingung dafür, dafs $f(z)$ eine Ambige enthält, auch noch auf eine etwas einfachere und zweckmäfsigere Weise ausdrücken. Da

die $h\lambda$te Potenz einer jeden Ambigen wirklich wird, so folgt, dafs wenn $f(z)$ eine Ambige $\phi(z)$ enthält, $f(z)^{h\lambda}$ sich in zwei wirkliche Faktoren zerlegen läfst, deren einer keinen der idealen Primfaktoren, der andere nur ideale Primfaktoren enthält, also:

$$(16.)\qquad f(z)^{h\lambda} = d(z)\cdot\Psi(z)$$

wo $\Psi(z) = \phi(z)^{h\lambda}$ ist, und $Nd(z)$ keine anderen Primfaktoren, als ϱ und die Primfaktoren der Determinante enthält. Diese Gleichung mit (15.) verbunden giebt:

$$(17.)\qquad \Psi(z)f(z_1) = \frac{\Delta(z)}{d(z)}\,\Phi(z)f(z).$$

Nimmt man auf beiden Seiten die Norm, und dividirt durch $Nf(\alpha)$, so hat man:

$$(18.)\qquad N\Psi(z) = N\left(\frac{\Delta(z)}{d(z)}\right) N\Phi(z).$$

Die Normen von $\Psi(z)$ und $\Phi(z)$ sind aber vollständig aus denselben idealen Faktoren zusammengesetzt, können sich also nur durch eine Einheit unterscheiden, welche eine Einheit in α sein mufs; dieselbe mufs auch einer nichtcomplexen Zahl congruent sein, nach dem Modul λ, weil die Normen der wirklichen Zahlen $\Psi(z)$ und $\Phi(z)$ diese Eigenschaft haben, und hieraus wird geschlossen, dafs diese Einheit nur eine λte Potenz sein kann. Man hat daher

$$(19.)\qquad N\left(\frac{\Delta(z)}{d(z)}\right) = e(\alpha)^{\lambda},$$

und folglich:

$$(20.)\qquad N\left(\frac{\Delta(z)}{e(\alpha)\,d(z)}\right) = 1.$$

Bezeichnet man diese gebrochene complexe Zahl, deren Norm gleich Eins ist, mit $e(z)$, und bildet den Ausdruck:

$$(21.)\qquad Pe(z) = 1 + e(z) + e(z)e(z_1) + \ldots + e(z)e(z_1)\ldots e(z_{\lambda-2}),$$

welcher selbst eine gebrochene Zahl in z ist, und darum in die Form

$$(22.)\qquad Pe(z) = \frac{A\cdot\delta(z)}{B}$$

gesetzt werden kann, so hat man vermöge der Grundeigenschaft dieses Ausdrucks, nach welcher

$$e(z)\,Pe(z_1) = Pe(z)\cdot$$

ist, die Gleichung:

$$(23.)\qquad \Delta(z)\,\delta(z_1) = e(\alpha)\,d(z)\,\delta(z).$$

Aus dieser Gleichung wird nun leicht gefolgert, dafs wenn $\delta(z)$ irgend einen idealen Primfaktor in z enthält, es zugleich auch alle seine conjugirten enthalten mufs, welche sich zu einem Primfaktor in α zusammensetzen. Wenn nämlich $p(z)$ ein idealer Primfaktor des $\delta(z)$ ist, so mufs $\delta(z_1)$ denselben ebenfalls enthalten, weil $\Delta(z)$ überhaupt keinen idealen Primfaktor in z enthält. Weil nun $\delta(z_1)$ den Primfaktor $p(z)$ enthält, so folgt, dafs $\delta(z)$ auch den Primfaktor $p(z_{-1})$ enthalten mufs, denselben mufs darum auch wieder $\delta(z_1)$ enthalten, und folglich $\delta(z)$ auch den Primfaktor $p(z_{-2})$ u. s. w. Setzt man nun den Werth des $\Delta(z)$ aus (23.) in (17.) ein, so hat man:

$$(24.)\qquad \Psi(z)\,f(z_1)\,\delta(z_1) = e(\alpha)\,\Phi(z)\,f(z)\,\delta(z).$$

Man kann nun $\delta(z)$, welches keine anderen idealen Faktoren in z enthält, als welche sich zu Faktoren der niederen Theorie in α zusammensetzen, mit $f(z)$ verbinden, ohne dafs dadurch die in $f(z)$ enthaltene Ambige wesentlich geändert wird. Schreibt man also einfach $f(z)$ statt $f(z)\,\delta(z)$, so hat man:

$$\Psi(z)\,f(z_1) = e(\alpha)\,\Phi(z)\,f(z),$$

und wenn mit $\Psi(z_1)\,\Psi(z_2)\,\ldots\ldots\,\Psi(z_{\lambda-1})$ multiplicirt wird:

$$N\Psi(z)f(z_1) = e(\alpha)\,\Phi(z)\,\Psi(z_1)\,\Psi(z_2)\,\ldots\,\Psi(z_{\lambda-1})\,f(z),$$

welche Gleichung in der einfacheren Form

$$(25.)\qquad L(\alpha)f(z_1) = M(z)f(z)$$

dargestellt werden kann, wo $M(z)$ eine wirkliche complexe Zahl in z ist, deren Norm ebenfalls keinen gemeinschaftlichen Faktor mit $\varrho D(\alpha)$ hat, und $L(\alpha)$ eine complexe Zahl in α, deren λte Potenz die Norm von $M(z)$ ist.

Dieser einfachen Gleichung (25.) also müssen alle wirklichen complexen Zahlen $f(z)$ genügen, welche Ambigen enthalten, und umgekehrt, jede wirkliche Zahl $f(z)$, welche einer solchen Gleichung genügt, enthält eine Ambige, wie man sogleich sieht, wenn man mit $f(z^{k^{\lambda-1}})$ multiplicirt, wodurch man auf die Bedingung des Satzes (II.) zurückkommt. Diejenigen Ambigen, welche sich nur durch ideale oder wirkliche Faktoren der niede-

ren Theorie unterscheiden, sind dabei nur als eine und dieselbe gerechnet. Man hat also folgenden Satz:

Wenn eine wirkliche complexe Zahl $f(z)$ einer Gleichung

$$L(\alpha)f(z_1) = M(z)f(z)$$

genügt, in welcher $L(\alpha)$ eine wirkliche complexe Zahl in α ist, die mit $\varrho D(\alpha)$ keinen gemeinschaftlichen Faktor hat, $M(z)$ eine wirkliche complexe Zahl in z, deren Norm keinen gemeinschaftlichen Faktor mit $\varrho D(\alpha)$ hat, so enthält $f(z)$ eine Ambige. Umgekehrt: wenn $f(z)$ eine Ambige enthält, so genügt es stets einer solchen Gleichung.

§. 9.

Darstellung der ambigen idealen Zahlen in z, als wirkliche complexe Zahlen in u, u_1, u_2 ....

Die wirkliche complexe Zahl $f(z)$, welche eine ideale Ambige enthalten soll, soll nun als eine complexe Zahl in w dargestellt werden. In dieser Form einer ganzen rationalen Funktion von w, des Grades $\lambda - 1$, tritt, wenn die Norm von $f(z)$ durch ϱ theilbar ist, eine Potenz von ϱ als gemeinschaftlicher Faktor aller Glieder heraus, auch wenn $f(z)$ in der Form einer linearen Funktion der Wurzeln z, z_1, ... $z_{\lambda-1}$ den Faktor ϱ nicht enthält. Man hat also:

$$f(z) = \varrho' f(w),$$

und demgemäfs auch

$$f(z_1) = \varrho' f(w\alpha),$$

und wenn diese Ausdrücke in die im Satz (III.) des vorigen Paragraphen gegebene Gleichung eingesetzt, und der Faktor ϱ' gehoben wird:

$$(1.) \qquad L(\alpha)f(w\alpha) = M(z)f(w).$$

Diese Gleichung kann nun anstatt der obigen als diejenige benutzt werden, welche alle idealen Ambigen gewährt, nämlich als in denjenigen wirklichen complexen Zahlen $f(w)$ enthalten, die dieser Gleichung genügen; denn die complexe Zahl $f(w)$ enthält genau dieselben idealen Primfaktoren, als $f(z)$, von welcher sie sich nur durch einen Faktor ϱ' unterscheidet.

In den folgenden Untersuchungen ist es nun vortheilhaft die Determinante $D(\alpha)$, welche der Theorie der complexen Zahlen in w und in z zu Grunde gelegt ist, einer neuen Beschränkung zu unterwerfen, welche darin besteht, dafs $(1-D(\alpha))$ durch ϱ theilbar sein soll, aber nicht durch ϱ^2. Diese Annahme über die Determinante soll hier, so wie in dem Folgenden überall gemacht werden.

Es sei nun

$$f(w) = A + A_1 w + A_2 w^2 + \dots + A_{\lambda-1} w^{\lambda-1},$$

sei ferner $M(z)$, in die Form einer complexen Zahl in w gesetzt:

$$M(z) = B + B_1 w + B_2 w^2 + \dots + B_{\lambda-1} w^{\lambda-1}.$$

Setzt man nun

$$M(z) f(w) = C + C_1 w + C_2 w^2 + \dots + C_{\lambda-1} w^{\lambda-1},$$

so hat man durch Ausführung der Multiplikation für die λ Coefficienten C, C_1, C_2 ... $C_{\lambda-1}$ ebensoviele Gleichungen, welche durch die eine

$$(2.) \quad \begin{aligned} C_k = {} & A_k B + A_{k-1} B_1 + \dots + A B_k + \\ & w^\lambda (A_{\lambda-1} B_{k+1} + \dots + A_{k+1} B_{\lambda-1}), \end{aligned}$$

für $k = 0, 1, 2, \dots \lambda - 1$, repräsentirt werden. Die Gleichung (1.) giebt daher unter den Coefficienten von $M(z)$ und $f(w)$ ein System von λ Gleichungen, welches durch die folgende repräsentirt wird:

$$(3.) \quad \begin{aligned} & A_k (B - \alpha^k L(\alpha)) + A_{k-1} B_1 + \dots + A B_k + \\ & w^\lambda (A_{\lambda-1} B_{k+1} + \dots + A_{k+1} B_{\lambda-1}) = 0, \end{aligned}$$

für $k = 0, 1, 2, \dots \lambda - 1$.

Ich mache nun aus diesem Systeme von λ Gleichungen ein System von Congruenzen, nach dem Modul ϱ^2. Die Coefficienten B, B_1, B_2, ... $B_{\lambda-1}$, als Coefficienten einer complexen Zahl in w, welche zugleich eine ganze complexe Zahl in z ist, müssen dem Systeme der Congruenzen (7.) §. 2. genügen, aus welchem unmittelbar folgt, erstens, dafs alle, mit Ausschlufs des ersten, durch ϱ theilbar sein müssen, und zweitens, dafs alle, mit Ausschlufs des ersten, unter einander congruent sein müssen, nach dem Modul ϱ^2. Die Gleichung (3.) giebt daher zunächst für den Modul ϱ die Congruenz:

$$(4.) \quad A_k (B - \alpha^k L(\alpha)) \equiv 0, \ \text{mod. } \varrho,$$

für $k=0, 1, 2, \ldots \lambda-1$, und weil A_k nicht für alle Werthe des k durch ϱ theilbar sein soll, so folgt hieraus, daſs

$$(5.)\qquad B \equiv L(\alpha), \text{ mod. } \varrho,$$

sein muſs. Ferner giebt die Gleichung (3.) nach dem Modul ϱ^2, weil

$$B_1 \equiv B_2 \equiv B_3 \ldots \equiv B_{\lambda-1}, \text{ mod. } \varrho^2$$

ist, die Congruenz:

$$A_k\,(B-\alpha^k L(\alpha)) +$$
$$B_1\,(A_{k-1}+A_{k-2}+\ldots+A+A_{\lambda-1}+\ldots+A_{k+1}), \text{ mod. } \varrho^2,$$

welche, wenn zum zweiten Theile $B_1 A_k$ addirt, und dasselbe vom ersten Theile subtrahirt wird, auch so dargestellt werden kann:

$$A_k\,(B-\alpha^k L(\alpha)-B_1)+B_1\,(A+A_1+\ldots+A_{\lambda-1}) \equiv 0, \text{ mod. } \varrho^2.$$

Setzt man nun, da $B-L(\alpha)$ und B_1 beide durch ϱ theilbar sind:

$$B-L(\alpha) \equiv c\varrho,\quad B_1 \equiv b\varrho, \quad \text{mod. } \varrho^2,$$

und beachtet, daſs $w^\lambda - 1$ durch ϱ theilbar, und

$$\alpha^k \equiv 1-k\varrho, \quad \text{mod. } \varrho^2,$$

ist, so hat man, wenn der gemeinschaftliche Faktor ϱ hinweggehoben wird:

$$(6.)\qquad A_k\,(kB+c-b)+b\,(A+A_1+\ldots+A_{\lambda-1}) \equiv 0, \text{ mod. } \varrho.$$

Ich setze nun erstens den Fall, es sei

$$A+A_1+A_2+\ldots+A_{\lambda-1} \equiv 0, \quad \text{mod. } \varrho,$$

so wäre auch:

$$(7.)\qquad A_k\,(kB+c-b) \equiv 0, \quad \text{mod. } \varrho,$$

für $k=0, 1, 2, \ldots \lambda-1$; weil nun B nicht durch ϱ theilbar ist, so kann die Congruenz $kB+c-b \equiv 0$, mod. ϱ, nur für einen Werth des k Statt haben, für alle übrigen Werthe des k müsste also A_k durch ϱ theilbar sein, und es müsste, weil die Summe aller Coefficienten $A, A_1, \ldots A_{\lambda-1}$ durch ϱ theilbar angenommen worden ist, sogar auch dieser eine Coefficient durch ϱ theilbar sein, also alle Coefficienten des $f(w)$ müssten einzeln durch ϱ theilbar sein, welches nicht Statt hat, weil bei der Verwandlung der complexen Zahl $f(z)$ in $f(w)$ aus letzterer ϱ^ν, als höchste Potenz von ϱ, welche sie enthalten kann, herausgehoben worden ist. Es folgt hieraus, daſs in einer Zahl $f(w)$, wel-

che der Gleichung (1.) genügt, die Summe ihrer Coefficienten nicht durch ϱ theilbar sein kann.

Die Congruenz

$$A + A_1 + A_2 + \dots + A_{\lambda-1} \equiv 0, \quad \text{mod. } \lambda,$$

enthält aber genau die nothwendige und hinreichende Bedingung dafür, dafs die Norm von $f(w)$ durch ϱ theilbar sei. Entwickelt man nämlich diese Norm, als Produkt der λ conjugirten Faktoren, und läfst alle Vielfachen von λ weg, so erhält man:

$$(8.) \qquad Nf(w) \equiv A^\lambda + A_1^\lambda w^\lambda + A_2^\lambda w^{2\lambda} + \dots + A_{\lambda-1}^\lambda w^{(\lambda-1)\lambda}, \quad \text{mod. } \lambda;$$

da nun $w^\lambda \equiv 1$, mod. ϱ, und da die λte Potenz einer jeden complexen Zahl in α dieser einfachen complexen Zahl congruent ist, nach dem Modul ϱ, so erhält man:

$$(9.) \qquad Nf(w) \equiv A + A_1 + A_2 + \dots + A_{\lambda-1}, \quad \text{mod. } \varrho.$$

Da man also anstatt der Bedingung, dafs die Summe der Coefficienten von $f(w)$ nicht durch ϱ theilbar sei, die setzen kann, dafs die Norm von $f(w)$ nicht durch ϱ theilbar sei, so hat man folgenden Satz:

(I.) Eine wirkliche complexe Zahl $f(w)$, deren Norm durch ϱ theilbar ist, ohne dafs $f(w)$ selbst durch ϱ theilbar ist, kann niemals eine Ambige enthalten.

Nimmt man nun zweitens in der Congruenz (6.)

$$A + A_1 + A_2 + \dots + A_{\lambda-1} \text{ nicht} \equiv 0, \quad \text{mod. } \varrho,$$

und bemerkt, dafs für einen bestimmten der λ Werthe des $k = 0, 1, 2, \dots \lambda - 1$

$$(10.) \qquad kB + c - b \equiv 0, \quad \text{mod. } \varrho,$$

sein mufs, so hat man aus der Congruenz (6.) nothwendig $b \equiv 0$, mod. ϱ, und hieraus folgt weiter, dafs A_k, für alle Werthe des $k \equiv 0, 1, 2, \dots \lambda - 1$, mit Ausschlufs des einen Werthes des k, welcher $kB + c - b \equiv 0$, mod. ϱ, giebt, durch ϱ theilbar sein mufs. Man hat daher folgenden Satz:

(II.) Wenn die wirkliche complexe Zahl $f(w)$ eine Ambige enthält, so müssen alle Coefficienten derselben, mit Ausschlufs eines einzigen, durch ϱ theilbar sein.

Es sollen nun die in der Determinante $D(\alpha)$ enthaltenen verschiedenen Primfaktoren in α in Betracht gezogen werden, welche mit $f(\alpha)$, $f_1(\alpha)$,

$f_2(\alpha)$ ... bezeichnet werden sollen, so dafs die Determinante, in ihre Primfaktoren zerlegt, folgenden Ausdruck hat:

$$(11.)\qquad D(\alpha) = E(\alpha) f(\alpha)^m f_1(\alpha)^{m_1} f_2(\alpha)^{m_2} \ldots,$$

in welchem $E(\alpha)$ eine Einheit bezeichnet. Es soll auch angenommen werden, dafs in diesem Ausdrucke die Faktoren $f(\alpha)^m$, $f_1(\alpha)^{m_1}$ u. s. w. nur wirkliche complexe Zahlen in α sind, durch welche Annahme die Primfaktoren $f(\alpha)$, $f_1(\alpha)$, ... keiner einschränkenden Bedingung unterworfen werden, sondern lediglich die Exponenten m, m_1, ..., da derselben z. B. immer dadurch genügt werden kann, dafs für alle diese Exponenten beliebige Vielfache der Klassenanzahl h genommen werden.

Macht man nun aus dem Systeme der λ Gleichungen bei (6.) ein System von Congruenzen, nach dem Modul $f(\alpha)^m$, indem bemerkt, dafs w^λ nach diesem Modul congruent Null ist, so hat man:

$$(12.)\qquad A_k\,(B - \alpha^k L(\alpha)) + A_{k-1} B_1 + \ldots + A B_k \equiv 0, \text{ mod. } f(\alpha)^m,$$

für $k = 0, 1, 2, \ldots \lambda - 1$.

Wenn nun angenommen wird, dafs von den Coefficienten des $f(w)$ die ersten n durch $f(\alpha)$ theilbar sind, der $(n+1)$te aber nicht theilbar, welches den Fall $n = 0$, wo der erste Coefficient A durch $f(\alpha)$ nicht theilbar ist, nicht ausschliefsen soll, so giebt die Congruenz (12.), für $k = n$, weil $A, A_1, \ldots A_{n-1}$ congruent Null sind:

$$(13.)\qquad A_n\,(B - \alpha^n L(\alpha)) \equiv 0, \quad \text{mod } f(\alpha),$$

und weil A_n nicht durch $f(\alpha)$ theilbar ist:

$$B - \alpha^n L(\alpha) \equiv 0, \quad \text{mod. } f(\alpha).$$

Es kann aber $B - \alpha^k L(\alpha)$ nur für diesen einen Werth $k = n$ durch $f(\alpha)$ theilbar sein, denn hätte man zugleich

$$B - \alpha^n L(\alpha) \equiv 0, \quad \text{und } B - \alpha^\nu L(\alpha) \equiv 0,$$

so würde daraus folgen:

$$(\alpha^n - \alpha^\nu) L(\alpha) \equiv 0, \quad \text{mod. } f(\alpha),$$

und hieraus:

$$L(\alpha) \equiv 0, \quad \text{mod. } f(\alpha),$$

welches unmöglich ist, weil $L(\alpha)$ keinen Faktor der Determinante enthält. Die Congruenz (12.) giebt nun für $k = 0, 1, 2, \dots n-1$,

$$
(13.)\quad \left.\begin{array}{l}
A(B-F(\alpha)) \equiv 0, \\
A_1(B-\alpha F(\alpha)) + AB_1 \equiv 0, \\
A_2(B-\alpha^2 F(\alpha)) + A_1 B_1 + AB_2 \equiv 0, \\
\vdots \\
A_{n-1}(B-\alpha^{n-1}F(\alpha)) + A_{n-2}B_1 + \dots + AB_{n-1} \equiv 0.
\end{array}\right\} \quad \text{mod.}\, f(\alpha)^m.
$$

Da $B - F(\alpha)$ nicht durch $f(\alpha)$ theilbar ist, so folgt aus der ersten dieser Congruenzen, daſs A den Faktor $f(\alpha)^m$ enthalten muſs. Hieraus, und weil auch $B - \alpha F(\alpha)$ nicht durch $f(\alpha)$ theilbar ist, ergiebt die zweite Congruenz, daſs A_1 durch $f(\alpha)^m$ theilbar sein muſs, und so fortschlieſsend erhält man:

$$A \equiv 0, \; A_1 \equiv 0, \; \dots\dots A_{n-1} \equiv 0, \quad \text{mod.}\, f(\alpha)^m.$$

Also wenn die ersten n Coefficienten durch $f(\alpha)$ theilbar sind, so müssen sie auch durch $f(\alpha)^m$ theilbar sein, und dieses für den einen Faktor der Determinante bewiesene Resultat gilt nothwendig eben so für alle anderen.

Ich setze nun:

$$
(14.)\quad \begin{array}{c}
u^\lambda = e(\alpha)f(\alpha)^m, \; u_1{}^\lambda = e_1(\alpha)f_1(\alpha)^{m_1}, \; u_2{}^\lambda = e_2(\alpha)f_2(\alpha)^{m_2} \dots \\
e(\alpha)e_1(\alpha)e_2(\alpha) \dots = E(\alpha),
\end{array}
$$

so ist:

$$D(\alpha) = u^\lambda \cdot u_1^\lambda \cdot u_2^\lambda \dots\dots$$

also:

$$w = u\, u_1\, u_2 \dots\dots$$

Wenn nun die ersten n Coefficienten des $f(w)$ durch $f(\alpha)$, also auch durch $f(\alpha)^m$, oder was dasselbe ist, durch u^λ theilbar sind, ferner die ersten n_1 Coefficienten theilbar durch $f_1(\alpha)$, also auch durch $f_1(\alpha)^{m_1}$, oder u_1^λ, u. s. w. und man setzt $u\, u_1\, u_2 \dots$ statt w, so hebt sich aus $f(w)$ der Faktor u^n, ebenso der Faktor $u_1{}^{n_1}$ u. s. w. heraus, und man hat:

$$(15.)\qquad f(w) = u^n\, u_1^{n_1}\, u_2^{n_2} \dots f(u, u_1, u_2 \dots),$$

wo $f(u, u_1, u_2 \dots)$ eine aus den Irrationalitäten $u, u_1, u_2 \dots$ gebildete complexe Zahl von folgender Form ist:

$$(16.)\qquad f(u, u_1, u_2 \ldots) = \Sigma_k A_k\, u^{|k-n|}\, u_1^{|k-n_1|}\, u_2^{|k-n_2|} \ldots.$$

wenn allgemein $|c|$ den kleinsten, nicht negativen Rest der Zahl c, nach dem Modul λ, bezeichnet. Die Bedingung, dafs in dem Ausdrucke des $f(w)$ der Coefficient A_n der erste nicht durch $f(\alpha)$ theilbare, der Coeffiicient A_{n_1} der erste nicht durch $f_1(\alpha)$ theilbare, u. s. w. sein soll, ergiebt für diesen Ausdruck der complexen Zahl $f(u, u_1, u_2 \ldots)$, dafs auch A_n nicht durch $f(\alpha)$, A_{n_1} nicht durch $f_1(\alpha)$, A_{n_2} nicht durch $f_2(\alpha)$ u. s. w. theilbar sein darf.

Die zu $f(u, u_1, u_2, \ldots)$ conjugirten complexen Zahlen erhält man, wenn man nur einer einzigen der Wurzelgröfsen $u, u_1, u_2, \ldots$ ihre λ Werthe giebt. Die Norm von $f(u, u_1, u_2 \ldots)$, als Produkt dieser λ conjugirten, ist alsdann eine, von den Irrationalitäten $u, u_1, u_2 \ldots$ vollständig freie, complexe Zahl in α. Vermöge der Bedingungen, dafs A_n nicht durch $f(\alpha)$, A_{n_1} nicht durch $f_1(\alpha)$ u. s. w. theilbar ist, kann diese Norm von $f(u, u_1, u_2 \ldots)$ keinen der Primfaktoren $f(\alpha)$, $f_1(\alpha)$, $f_2(\alpha) \ldots$ enthalten. Um diefs zu beweisen, bemerke ich, dafs in dem Ausdrucke (16.) das $n$te Glied, welches $u^{|n-n|}$, also nur u^0 enthält, das einzige Glied ist, welches u nicht enthält, und dafs demgemäfs in der Norm von $f(u, u_1, u_2 \ldots)$, in welcher u selbst nicht mehr vorkommt, sondern nur noch u^λ, die λte Potenz dieses $n$ten Gliedes das einzige Glied sein mufs, welches u^λ nicht enthält, dafs also:

$$Nf(u, u_1, u_2 \ldots) \equiv A_n^\lambda\, u_1^{|n-n_1|\lambda}\, u_2^{|n-n_2|\lambda} \ldots \quad \text{mod. } u^\lambda,$$

und weil A_n, u_1^λ, u_2^λ, ... den Faktor $f(\alpha)$ nicht enthalten, dafs diese Norm den Faktor $f(\alpha)$ nicht enthält. In derselben Weise wird gezeigt, dafs sie auch keinen der übrigen Faktoren der Determinante enthalten kann.

Da nun zuerst im §. 8. gezeigt worden ist, dafs jede ideale Ambige in einer wirklichen Zahl $f(z)$ als Complex aller idealen Primfaktoren enthalten ist, so dafs die Norm dieser Zahl $f(z)$ aufser der Norm der in ihr enthaltenen Ambigen nur noch die Primfaktoren der Determinante und eine Potenz von ϱ enthalten kann; da ferner in dem gegenwärtigen Paragraphen gezeigt worden ist, dafs, wenn diese, die Ambige enthaltende Zahl $f(z)$ als complexe Zahl in w dargestellt, und von einer Potenz von ϱ, welche in dieser Form als gemeinschaftlicher Faktor aller ihrer Coefficienten heraustreten kann, befreit wird, aus derselben eine complexe Zahl $f(w)$ entsteht, deren

Norm nicht mehr ϱ enthält; da endlich gezeigt worden ist, daſs diese die Ambige enthaltende Zahl $f(w)$ durch Einführung der Wurzeln $u, u_1, u_2 \ldots$, und nachdem die Potenzen von $u, u_1, u_2, \ldots$, welche dabei als gemeinschaftliche Faktoren aller Glieder heraustreten, entfernt werden, eine wirkliche complexe Zahl $f(u, u_1, u_2, \ldots)$ ergiebt, deren Norm keinen Faktor der Determinante weiter enthält: so folgt, daſs $f(u, u_1, u_2 \ldots)$ die in $f(z)$ enthaltene Ambige nicht nur ebenfalls enthält, sondern daſs sie als diese Ambige selbst angesehen werden muſs, welche somit als ideale Zahl in z, in der Theorie der complexen Zahlen in $u, u_1, u_2 \ldots$ als wirkliche complexe Zahl dargestellt werden kann. Also:

(III.) Jede ideale Ambige in z läſst sich als eine wirkliche complexe Zahl von der Form $f(u, u_1, u_2 \ldots)$ darstellen, welche so beschaffen ist, daſs sie durch Multiplikation mit $u^n u_1^{n_1} u_2^{n_2} \ldots$, wenn die Exponenten $n, n_1, n_2 \ldots$ passend bestimmt werden, in eine complexe Zahl in w übergeht.

§. 10.

Untersuchung aller wirklichen complexen Zahlen in $u, u_1, u_2, \ldots$, welche ideale ambige Zahlen in z darstellen.

Die in den vorhergehenden Paragraphen bewiesenen Sätze gewähren die Mittel, alle idealen Ambigen in der Theorie der complexen Zahlen in z zu finden, und zwar in der Form von wirklichen complexen Zahlen, welche aus den Wurzeln $u, u_1, u_2 \ldots$ gebildet sind. Als den einfachsten Weg zu diesem Ziele zu gelangen, wähle ich den, zunächst alle wirklichen Zahlen $f(w)$ zu finden, welche einer Gleichung von der Form (1.) §. 9:

$$(1.) \qquad L(\alpha) f(w\alpha) = M(z) f(w)$$

genügen, in welcher Gleichung vorläufig in $L(\alpha)$ und in $NM(z)$ die Faktoren der Determinante $f(\alpha), f_1(\alpha), \ldots$ zugelassen werden sollen, der Faktor ϱ aber ausgeschlossen sein soll. Diese Aufgabe läſst sich folgendermaaſsen aussprechen:

Alle wirklichen complexen Zahlen $f(w)$ zu finden, welche der Bedingung genügen, daſs $\frac{f(w\alpha)}{f(w)}$ als eine gebrochene, wirkliche complexe Zahl

in z sich darstellen lasse, in der Art, dafs die Norm des Nenners nicht durch ϱ theilbar sei.

Zunächst ist klar, dafs wenn $f(w)$ dieser Bedingung genügt, auch $w^k f(w)$ derselben genügen mufs, für jeden Werth des k. Da nun oben §. 9. im Satze (II.) bewiesen worden ist, dafs in einer jeden Zahl $f(w)$, welche den Bedingungen der vorliegenden Aufgabe genügt, alle Coefficienten, mit Ausschlufs eines einzigen, durch ϱ theilbar sein müssen, so kann man durch Multiplikation mit einer passenden Potenz von w das Glied, welches diesen Coefficienten hat, zum ersten Gliede machen, d. h. zu dem Gliede, welches die irrationale Wurzel w nicht enthält, wodurch $f(w)$ die Form

$$f(w) = C + \varrho\psi(w) \tag{2.}$$

erhält, wo C eine durch ϱ nicht theilbare complexe Zahl in α ist, welche auch als nichtcomplexe ganze Zahl angenommen werden kann. Es reicht also hin, nur die in dieser Form enthaltenen, der Aufgabe genügenden Zahlen $f(w)$ zu finden.

Ferner folgt unmittelbar, wenn $f(w)$ der Aufgabe genügt, dafs auch $f(w)\ F(z)$ derselben genügen mufs, wenn $F(z)$ eine wirkliche complexe Zahl in z ist, deren Norm nicht durch ϱ theilbar ist.

Endlich ergiebt sich auch sehr leicht, dafs wenn $f(w)$ der Aufgabe genügt, ebenso alle complexen Zahlen in w, welche congruent $f(w)$ sind, nach dem Modul λ, der Aufgabe genügen müssen; denn es ist:

$$f(w) + \lambda g(w) = f(w)\left(1 + \frac{\lambda g(w)}{f(w)}\right),$$

und wenn man den Bruch $\frac{g(w)}{f(w)}$ in die Form bringt, dafs sein Nenner eine complexe Zahl in α wird, also:

$$\frac{g(w)}{f(w)} = \frac{G(w)}{F(\alpha)},$$

und bemerkt, dafs nach dem Satze (I.) §. 2 $\lambda G(w)$ eine ganze complexe Zahl in z ist, so hat man:

$$f(w) + \lambda g(w) = \frac{f(w)\,\Phi(z)}{F(\alpha)}, \tag{3.}$$

wo $N\Phi(z)$ nicht durch ϱ theilbar ist, also:

$$(4.)\qquad \frac{f(w\alpha)+\lambda g(w\alpha)}{f(w)+\lambda g(w)} = \frac{f(w\alpha)\,\Phi(z_1)}{f(w)\,\Phi(z)},$$

woraus die Richtigkeit der aufgestellten Behauptung erhellt.

Da hiernach nur alle nach dem Modul λ incongruenten Zahlen $f(w)$ von der Form $C+\varrho\psi(w)$ zu suchen sind, welche den Bedingungen der Aufgabe genügen, so wird es zweckmäfsig sein, bei dieser Untersuchung die Logarithmen der complexen Zahlen, nach dem Modul λ, anstatt dieser complexen Zahlen selbst anzuwenden, in ähnlicher Weise, wie ich dieselben schon früher für die Theorie der complexen Zahlen in α mit Erfolg angewendet habe.

Zunächst ist zu bemerken, dafs eine jede Zahl von der Form $C+\varrho\psi(w)$ stets auf verschiedene Weisen in diese Form gesetzt werden kann, da man dem $\psi(w)$ beliebig eine complexe Zahl in α hinzufügen kann, wenn man dafür das ϱfache derselben von C hinwegnimmt. Um diese Willkürlichkeit auszuschliefsen, setze ich fest: es soll $\psi(w)$ in dieser Form stets so gewählt werden, dafs es für $w=1$ gleich Null wird, welches immer geleistet werden kann, indem man von $\psi(w)$ die Summe aller seiner Coefficienten abzieht, und das ϱfache dieser Summe dem C zulegt.

Ich entwickele nun den Logarithmus

$$(5.)\qquad l\left(\frac{f(w)}{C}\right) = l\left(1+\frac{\varrho\psi(w)}{C}\right)$$

so nach Potenzen von ϱ, dafs in dieser Entwickelung alle diejenigen Glieder, welche Vielfache von λ werden, wegfallen. Das $k$te Glied der Entwickelung dieses Logarithmus ist:

$$\frac{-(-1)^k \varrho^k \psi(w)^k}{k\,C^k}.$$

Da nun $\varrho^{\lambda-1}$ ein Vielfaches von λ ist, so folgt, dafs das $\lambda-1$te Glied wegfällt, so wie auch alle folgenden, insofern sie nicht λ auch im Nenner enthalten, also insofern nicht k durch λ theilbar ist. Wenn aber k ein Vielfaches von λ ist, so nehme man $k=m\lambda^n$, wo m nicht weiter durch λ theilbar sein soll; man hat alsdann $\varrho^{m\lambda^n} = \varrho^{m\lambda^{n-1}(\lambda-1)}\,\varrho^{m\lambda^{n-1}}$, also theilbar durch $\lambda^{m\lambda^{n-1}}$, und demnach mufs $\frac{1}{k}\varrho^k$ für einen solchen Werth des k den Faktor λ mindestens $m\lambda^{n-1}-n$ mal enthalten. Diese Anzahl ist aber stets gröfser alsEins, aufser in dem einen Falle, wo zugleich $n=1$ und $m=1$, also $k=\lambda$

ist. Von allen Gliedern dieser Entwickelung des Logarithmus bleiben also nur die ersten $\lambda - 2$, und aufserdem das λte Glied, welches den Faktor $\frac{1}{\lambda}\varrho^\lambda$ hat, der bekanntlich gleich ϱ, multiplicirt mit einer Einheit ist. Man hat daher:

$$(6.)\quad l\left(\frac{f(w)}{C}\right) \equiv \frac{\varrho\psi(w)}{1\cdot C} - \frac{\varrho^2\psi(w)^2}{2\cdot C^2} + \ldots + \frac{\varrho^{\lambda-2}\psi(w)^{\lambda-2}}{(\lambda-2)\,C^{\lambda-2}} + K,\ \text{mod.}\,\lambda,$$

wo der Kürze wegen

$$K = \frac{\varrho E(\alpha)\,\psi(w)^\lambda}{C^\lambda}$$

gesetzt ist. Denkt man sich nun diesen ganzen Ausdruck nach den Potenzen von w entwickelt, und als ganze rationale Funktion von w des $\lambda - 1$ten Grades dargestellt; denkt man sich ferner die Brüche, deren Nenner die Potenzen von C sind, durch die ganzen Zahlen ersetzt, welchen sie congruent sind, nach dem Modul λ; setzt man alsdann überall $1 - \varrho$ für α, und ordnet nach Potenzen von ϱ; setzt man endlich $1 - v$ statt w und ordnet das, was in die einzelnen Potenzen des ϱ multiplicirt ist, nach Potenzen von v: so erhält man eine Entwickelung von folgender Form:

$$(7.)\quad l\left(\frac{f(w)}{C}\right) \equiv \varrho\psi_1(v) + \varrho^2\psi_2(v) + \ldots + \varrho^{\lambda-2}\psi_{\lambda-2}(v),\ \text{mod.}\ \lambda,$$

in welcher $\psi_1(v)$, $\psi_2(v)$ u. s. w. ganze rationale Funktionen von v, vom Grade $\lambda - 1$ sind, mit nichtcomplexen ganzen Zahlen als Coefficienten. Von der ersten derselben $\psi_1(v)$ insbesondere ist noch zu bemerken, dafs für $v = 0$ auch $\psi_1(v) = 0$ werden mufs, vermöge der Festsetzung, dafs in $f(w) = C + \varrho\psi(w)$, für $w = 1$, $\psi(w) = 0$ sein soll.

Wenn nun die logarithmische Entwickelung einer complexen Zahl der Form $C + \varrho\psi(w)$ nach den angegebenen Regeln gebildet ist, so ist sie nach dem Modul λ eine vollständig bestimmte, d. h. eine gegebene complexe Zahl hat nur eine Entwickelung ihres Logarithmus, nach dem Modul λ. Wenn nun aber umgekehrt die logarithmische Entwickelung gegeben ist, so ist die Frage: in wie weit dadurch die complexe Zahl selbst bestimmt ist. Um diefs zu untersuchen, gehe ich von dem ganz speciellen Falle aus, wo die logarithmische Entwickelung congruent Null ist, also

$$(8.)\quad l\left(\frac{f(w)}{C}\right) \equiv l\left(\frac{C + \varrho\psi w}{C}\right) \equiv 0,\quad \text{mod.}\ \lambda.$$

In diesem Falle hat man aus der Congruenz (6.), wenn man dieselbe zunächst nur für den Modul ϱ^2 betrachtet:

$$0 \equiv \varrho\psi(w), \quad \text{mod. } \varrho^2,$$

also $\psi(w)$ durch ϱ theilbar. Setzt man nun $\psi(w) = \varrho\chi_1(w)$, und betrachtet die Congruenz (6.) nach dem Modul ϱ^3, so ergiebt sie, dafs $\chi_1(w)$ weiter durch ϱ theilbar sein mufs, also $\psi(w)$ theilbar durch ϱ^2, so fortschliefsend erhält man zuletzt: $\psi(w)$ theilbar durch $\varrho^{\lambda-2}$, also $\varrho\psi(w)$ ein Vielfaches von λ, d. h. die logarithmische Entwickelung von $f(w)$ ist nur dann congruent Null, wenn $f(w)$ einer complexen Zahl in α congruent ist, nach dem Modul λ. Wenn nun die logarithmischen Entwickelungen zweier Zahlen $f(w)$ und $f'(w)$ congruent sind, also der Unterschied derselben congruent Null, so hat man

$$l\left(\frac{f(w)}{C}\right) - l\left(\frac{f'(w)}{C'}\right) \equiv 0, \quad \text{mod. } \lambda,$$

also

$$l\left(\frac{C'f(w)}{Cf'(w)}\right) \equiv 0, \quad \text{mod. } \lambda,$$

woraus folgt, dafs $\frac{C'f(w)}{Cf'(w)}$ einer complexen Zahl in α congruent sein mufs, nach dem Modul λ, oder was dasselbe ist: $Af(w) \equiv f'(w)$, mod. λ, wo A eine complexe Zahl in α ist.

Nachdem diese allgemeinen Eigenschaften der logarithmischen Entwickelungen der complexen Zahlen von der Form $C + \varrho\psi(w)$ festgestellt sind, wende ich dieselben zum Zwecke der Lösung der vorliegenden Aufgabe an. Ich verwandle in der Congruenz (7.) w in $w\alpha$, wodurch $v = 1 - w$ in $1 - w\alpha = v + \varrho(1 - v)$ übergeht, entwickele die rationalen Funktionen von $v + \varrho(1 - v)$ nach dem Taylorschen Satze nach Potenzen von ϱ, und ziehe die unveränderte Congruenz (7.) von diesen ab, so ist:

$$\text{(9.)} \quad l\left(\frac{f(w\alpha)}{f(w)}\right) \equiv \varrho^2(1-v)\psi_1'(v) + \frac{\varrho^3(1-v)^2\psi_1''(v)}{1.\,2.} + \frac{\varrho^4(1-v)^3\psi_1'''(v)}{1.\,2.\,3.} + \dots$$
$$+ \varrho^3(1-v)\psi_2'(v) + \frac{\varrho^4(1-v)^2\psi_2''(v)}{1.\,2.} + \dots$$
$$+ \varrho^4(1-v)\psi_3'(v) + \dots$$

Ich entwickele nun den Logarithmus der complexen Zahl $\frac{M(z)}{L(\alpha)}$, welche nach den Bedingungen der Aufgabe gleich $\frac{f(w\alpha)}{f(w)}$ werden soll. Setzt

man $M(z)$ zunächst in die Form einer complexen Zahl in w, so hat man, wie im §. 2 gezeigt worden:

$$(10.)\quad M(z) = G + G_1(1-w) + G_2(1-w)^2 + \dots + G_{\lambda-1}(1-w)^{\lambda-1},$$

wo $G_{\lambda-1}$ durch ϱ, $G_{\lambda-2}$ durch ϱ^2, $G_{\lambda-3}$ durch ϱ^3 etc. theilbar ist. Dividirt man durch $L(\alpha)$, ersetzt die Brüche, mit dem Nenner $L(\alpha)$ durch die ganzen complexen Zahlen, denen sie nach dem Modul λ congruent sind, nimmt ferner $1 - w = v$ und $1 - \alpha = \varrho$ und ordnet nach Potenzen von ϱ, so hat man:

$$(11.)\quad \frac{M(z)}{L(\alpha)} \equiv 1 + \mathfrak{b}_1 v^{\lambda-1}\varrho + (\mathfrak{a}_2 + \mathfrak{b}_2 v^{\lambda-1}\mathfrak{c}_2 v^{\lambda-2}) + \\ + (\mathfrak{a}_3 + \mathfrak{b}_3 v^{\lambda-1} + \mathfrak{c}_3 v^{\lambda-2} + \mathfrak{d}_3 v^{\lambda-3})\varrho^3 + \dots$$

nach dem Modul λ, wo $\mathfrak{b}_1$, $\mathfrak{a}_2$, $\mathfrak{b}_2$, $\mathfrak{a}_3$ u. s. w. nichtcomplexe ganze Zahlen sind. Hieraus erhält man nach der obigen Methode folgende Form der Entwickelung des Logarithmus:

$$(12.)\quad l\left(\frac{M(z)}{L(\alpha)}\right) \equiv \mathfrak{B}_1 v^{\lambda-1}\varrho + (\mathfrak{A}_2 + \mathfrak{B}_2 v^{\lambda-1} + \mathfrak{C}_2 v^{\lambda-2})\varrho^2 + \\ + (\mathfrak{A}_3 + \mathfrak{B}_3 v^{\lambda-1} + \mathfrak{C}_3 v^{\lambda-2} + \mathfrak{D}_3 v^{\lambda-3})\varrho^3 + \dots$$

nach dem Modul λ, wo $\mathfrak{B}_1$, $\mathfrak{A}_2$, $\mathfrak{B}_2$ u. s. w. ebenfalls nichtcomplexe ganze Zahlen sind. Weil nun

$$\frac{f(w\alpha)}{f(w)} = \frac{M(z)}{L(\alpha)}$$

sein soll, so mufs der Logarithmus der einen dieser complexen Zahlen dem Logarithmus der anderen congruent sein. Die Vergleichung der einzelnen Glieder beider Entwickelungen ergiebt folgende Congruenzen:

$$(13.)\quad \begin{aligned} &(1-v)\psi_1'(v) \equiv \mathfrak{A}_2 + \mathfrak{B}_2 v^{\lambda-1} + \mathfrak{C}_2 v^{\lambda-2} \\ &(1-v)\psi_2'(v) + \frac{(1-v)^2\psi'(v)}{1.\,2.} \equiv \mathfrak{A}_3 + \mathfrak{B}_3 v^{\lambda-1} + \mathfrak{C}_3 v^{\lambda-2} + \mathfrak{D}_3 v^{\lambda-3} \\ &(1-v)\psi_3'(v) + \frac{(1-v)^2\psi_1''(v)}{1.\,2.} + \frac{(1-v)^3\psi_1'''(v)}{1.\,2.\,3} \\ &\qquad\qquad \equiv \mathfrak{A}_4 + \mathfrak{B}_4 v^{\lambda-1} + \mathfrak{C}_4 v^{\lambda-2} + \mathfrak{D}_4 v^{\lambda-3} + \mathfrak{E}_4 v^{\lambda-4} \end{aligned}$$

u. s. w., nach dem Modul λ. Setzt man nun

$$\Psi_1(v) = \alpha_1 v + \alpha_2 v^2 + \dots + \alpha_{\lambda-1} v^{\lambda-1},$$

so hat man

$$(14.)\qquad (1-v)\psi'_1(v) = a_1 + (2a_2 - a_1)v + (3a_3 - 2a_2)v^2 + \\ \dots - (\lambda-1)a_{\lambda-1}v^{\lambda-1},$$

und weil vermöge der ersten der Congruenzen (13.) die Glieder dieses Ausdrucks, welche v, v^2, ... $v^{\lambda-3}$ enthalten, congruent Null sein müssen, so hat man:

$$2a_2 - a_1 \equiv 0,\ 3a_3 - 2a_2 \equiv 0,\ \dots (\lambda-2)a_{\lambda-2} - (\lambda-3)a_{\lambda-3} \equiv 0,$$

woraus unmittelbar folgt:

$$a_1 \equiv \frac{c_1}{1},\quad a_2 \equiv \frac{c_1}{2},\quad a_3 \equiv \frac{c_1}{3} \dots a_{\lambda-2} \equiv \frac{c_1}{\lambda-2},$$

so dafs man für $\psi_1(v)$ folgenden Ausdruck erhält:

$$(15.)\qquad \psi_1(v) \equiv c_1\left(\frac{v}{1} + \frac{v^2}{2} + \frac{v^3}{3} + \dots + \frac{v^{\lambda-1}}{\lambda-1}\right) + B_1 v^{\lambda-1},$$

wo c_1 und B_1 beliebige ganze Zahlen sind. Mit Hülfe dieses gefundenen Ausdrucks des $\psi_1(v)$ findet man aus der zweiten der Congruenzen (13.) ohne Schwierigkeit folgenden Ausdruck des $\psi_2(v)$:

$$(16.)\qquad \psi_2(v) \equiv c_2\left(\frac{v}{1} + \frac{v^2}{2} + \dots + \frac{v^{\lambda-1}}{\lambda-1}\right) + A_2 + B_2 v^{\lambda-1} + C_2 v^{\lambda-2},$$

wo c_2, A_2, B_2, C_2 beliebige ganze Zahlen sind. Ebenso findet man weiter aus der dritten der Congruenzen (13.):

$$(17.)\qquad \psi_3(v) \equiv c_3\left(\frac{v}{1} + \frac{v^2}{2} + \dots + \frac{v^{\lambda-1}}{\lambda-1}\right) \\ + A_3 + B_3 v^{\lambda-1} + C_3 v^{\lambda-2} + D_3 v^{\lambda-3}.$$

Allgemein hat $\psi_k(v)$ nach den Congruenzen (13.) einen Ausdruck, welcher sich von den hier für $k = 1, 2, 3$ gegebenen nur dadurch unterscheidet, dafs die Glieder, welche dem ersten Theile hinzuzufügen sind, bis zu dem Gliede mit $v^{\lambda-k}$ einschliefslich gehen. Setzt man nun der Kürze wegen:

$$W \equiv \frac{v}{1} + \frac{v^2}{2} + \frac{v^3}{3} + \dots + \frac{v^{\lambda-1}}{\lambda-1},$$

so hat man vermöge der gefundenen Ausdrücke der $\psi_1(v)$, $\psi_2(v)$ u. s. w.

$$(18.)\qquad l\left(\frac{f(\alpha)}{C}\right) \equiv (c_1\varrho + c_2\varrho^2 + \dots + c_{\lambda-2}\varrho^{\lambda-2})W + B_1 v^{\lambda-1}\varrho + \\ + (A_2 + B_2 v^{\lambda-1} + C_2 v^{\lambda-2})\varrho^2 + (A_3 + B_3 v^{\lambda-1} + C_3 v^{\lambda-2} + D_3 v^{\lambda-3})\varrho^3 + \dots$$

Vergleicht man den Ausdruck auf der rechten Seite dieser Congruenz, welcher auf das erste Glied folgt, mit der Congruenz (12.), so erkennt man,

dafs derselbe den Logarithmus einer complexen Zahl in z darstellt. Man hat daher:

$$(19.) \quad l\left(\frac{f(w)}{C}\right) \equiv (c_1\varrho + c_2\varrho^2 + \dots + c_{\lambda-2}\varrho^{\lambda-2})W + l\left(\frac{F(z)}{F(\alpha)}\right), \text{ mod. } \lambda,$$

als nothwendige Bedingung dafür, dafs die Zahl $f(w)$ eine Gleichung von der Form

$$L(\alpha)f(w\alpha) = M(z)f(w)$$

genüge, in welcher $NM(z)$ und $L(\alpha)$ nicht durch ϱ theilbar sind. Dafs diese Bedingung auch eine hinreichende ist, folgt daraus, dafs wenn w in $w\alpha$ verwandelt wird, also v in $v + \varrho\,(1 - v)$, und von der so veränderten Congruenz (19.) die unveränderte abgezogen wird, der Logarithmus von $\frac{f(w\alpha)}{f(w)}$ in der That congruent dem Logarithmus einer complexen Zahl in z gefunden wird. Von dem mit W bezeichneten Ausdrucke bemerke ich noch, dafs derselbe, wenn $v = 1 - w$ gesetzt wird, und man nach Potenzen von w ordnet, in einen Ausdruck derselben Form übergeht, oder dafs

$$(20.) \quad W \equiv \frac{w}{1} + \frac{w^2}{2} + \frac{w^3}{3} + \dots + \frac{w^{\lambda-1}}{\lambda-1}, \text{ mod. } \lambda.$$

Vergleicht man den Ausdruck (19.) des Logarithmus einer der Gleichung (1.) genügenden Zahl $f(w)$ mit dem Ausdrucke (12.) des Logarithmus einer complexen Zahl in z, so erkennt man sogleich, dafs, wenn $f(w)$ eine complexe Zahl in z sein soll, nothwendig die $\lambda - 2$ Zahlen c_1, c_2, ... $c_{\lambda-2}$ alle congruent Null sein müssen, mod. λ; denn die Glieder $c_1\varrho v$, $c_2\varrho^2 v$, ... $c_{\lambda-2}\varrho^{\lambda-2} v$, welche im Logarithmus von $f(w)$ enthalten sind, kommen in dem Logarithmus einer complexen Zahl in z nicht vor. Umgekehrt, wenn c_1, c_2 ... $c_{\lambda-2}$ alle congruent Null sind, mod. λ, so ist der Logarithmus von $f(w)$ derselbe, als der Logarithmus einer complexen Zahl in z, und darum $f(w) \equiv A\,F(z)$, mod. λ, oder $f(w) = A\,F(z) + \lambda G(w)$, also weil $\lambda G(w)$ eine complexe Zahl in z ist, ist $f(w)$ nothwendig eine complexe Zahl in z.

Wenn nun zwei Zahlen $f(w)$ und $f'(w)$, welche beide den Bedingungen der Aufgabe genügen, in ihren Logarithmen dieselben Werthe der Zahlen c_1, c_2 ... $c_{\lambda-2}$ haben, nach dem Modul λ, so giebt die Differenz ihrer Logarithmen, also der Logarithmus ihres Quotienten, den Logarithmus einer complexen Zahl in z, und man hat:

$$(21.)\qquad l\left(\frac{C'f'(w)}{Cf(w)}\right) \equiv l\left(\frac{F(z)}{M}\right), \text{ mod. } \lambda.$$

Hieraus folgt, wie oben gezeigt worden, dafs die eine complexe Zahl der anderen, multiplicirt mit einer complexen Zahl in α, congruent sein mufs, also:

$$(22.)\qquad \frac{f'(w)}{f(w)} \equiv \frac{AF(z)}{M}, \text{ mod. } \lambda.$$

Macht man nun aus dieser Congruenz eine Gleichung, indem man das λfache einer complexen Zahl in w hinzufügt, welches ebenfalls eine complexe Zahl in z ist, so erhält man:

$$(23.)\qquad f'(w) = \frac{f(w)\,F'(z)}{M'},$$

wo $F'(z)$ eine ganze complexe Zahl in z, M' eine ganze complexe Zahl in α ist, welche den Faktor ϱ nicht enthält. Die eine dieser beiden Zahlen $f(w)$ und $f'(w)$ entsteht also aus der anderen durch Multiplikation mit einer gebrochenen complexen Zahl in z, deren Nenner kein ϱ enthält. Umgekehrt, wenn $f(w)$ und $f'(w)$ in dieser durch die Gleichung (23.) ausgedrückten Beziehung zu einander stehen, so hat man

$$(24.)\qquad l\left(\frac{f'(w)}{C'}\right) - l\left(\frac{f(w)}{C}\right) \equiv \frac{lF'(z)}{M'}, \text{ mod. } \lambda,$$

woraus folgt, dafs die Logarithmen von $f(w)$ und von $f'(w)$ dieselben Werthe der Zahlen $c_1, c_2, \dots c_{\lambda-1}$ haben müssen, nach dem Modul λ.

Es kann nun eine jede der $\lambda-2$ Zahlen $c_1, c_2, \dots c_{\lambda-2}$ die λ verschiedenen Werthe $0, 1, 2, \dots \lambda-1$ erhalten, die Anzahl aller verschiedenen Werthverbindungen dieser Zahlen, und nur diese, geben aber solche der Aufgabe genügende Zahlen $f(w)$, welche sich nicht durch Multiplikation mit complexen Zahlen in z eine aus der andern erzeugen lassen. Dieses Resultat giebt folgenden Satz:

Es giebt genau $\lambda^{\lambda-2}$ ursprüngliche complexe Zahlen $f(w)$, welche der Bedingung genügen, dafs $\frac{f(w\alpha)}{f(w)}$ einer gebrochenen complexen Zahl in z gleich sei, deren Nenner ϱ nicht enthält, welche in der Art von einander unabhängig sind, dafs keine aus einer anderen durch Multiplikation mit einer gebrochenen complexen Zahl in z, deren Nenner ϱ nicht enthält, erzeugt werden kann.

§. 11.

Anzahl der wesentlich verschiedenen Ambigen.

Aus den Zahlen $f(w)$, welche der im vorigen Paragraphen gestellten und gelösten Aufgabe genügen, sollen nun die Ambigen selbst, als wirkliche complexe Zahlen in u, u_1, u_2 ... hergeleitet werden.

Es sei

$$(1.)\qquad f(w) = C + \varrho C_1 w + \varrho C_2 w^2 + \dots + \varrho C_{\lambda-1} w^{\lambda-1}$$

irgend eine der $\lambda^{\lambda-2}$ complexen Zahlen, welche als ursprüngliche Lösungen der Aufgabe bezeichnet worden sind, so ist $f(w) + \lambda g(w)$ ebenfalls eine der Aufgabe genügende Zahl, aber eine solche, welche aus der ursprünglichen $f(w)$ durch Multiplikation mit einer wirklichen complexen Zahl in z entsteht, und man hat:

$$(2.)\ f(w) + \lambda g(w) = C + \lambda B + (\varrho C_1 + \lambda B_1)\, w + (\varrho C_2 + \lambda B_2)\, w^2 + \dots.$$

In dieser complexen Zahl kann und soll nun über die Zahlen B, B_1, B_2, ... $B_{\lambda-1}$ so verfügt werden, dafs die n ersten Glieder durch u^λ, d. h. durch $f(\alpha)^m$ theilbar werden, das $n+1$ te Glied aber nicht durch $f(\alpha)$ theilbar, ferner dafs die ersten n_1 Glieder durch u_1^λ, d. i. durch $f_1(\alpha)^{m_1}$ theilbar werden, das $n_1 + 1$ te Glied aber nicht durch $f_1(\alpha)$ theilbar; ferner dafs die n_2 ersten Glieder durch u_2^λ, d. i. $f_2(\alpha)^{m_2}$ theilbar werden, das $n_2 + 1$ te Glied aber nicht durch $f_2(\alpha)$ theilbar u. s. f. Setzt man alsdann für w seinen Werth $w = u\, u_1\, u_2 \dots$, so kann man die Faktoren u^n, $u_1^{n_1}$, $u_2^{n_2}$ ... heraus heben, und erhält so:

$$(3.)\qquad f(w) + \lambda g(w) = u^n\, u_1^{n_1}\, u_2^{n_2} \dots f(u, u_1, u_2, \dots).$$

Es ist nun, wie im §. 9. gezeigt worden, $f(u, u_1, u_2, \dots)$ eine complexe Zahl in u, u_1, u_2 ..., deren Norm keinen Faktor der Determinante $D(\alpha)$ enthält, und auch nicht durch ϱ theilbar ist, welche also eine Ambige selbst darstellt, nämlich die in $f(w) + \lambda g(w)$ enthaltene Ambige, und welche einer Gleichung von der Form

$$(4.)\qquad L(\alpha) f(u\alpha, u_1, u_2 \dots) = M(z) f(u, u_1, u_2 \dots)$$

genügt, in der $L(\alpha)$ und $NM(z)$ keinen Faktor der Determinante und kein ϱ enthalten.

Wenn nun die Anzahl der in der Determinante $D(\alpha)$ enthaltenen verschiedenen Primfaktoren $f(\alpha)$, $f_1(\alpha)$ u. s. w. gleich r ist, so hat man r Zahlen $n, n_1, n_2, \ldots n_{r-1}$, denen man einzeln alle Werthe $0, 1, 2, \ldots \lambda - 1$ geben kann, welche also λ^r verschiedene Werthverbindungen zulassen. Man erhält also aus jeder der $\lambda^{\lambda-2}$ ursprünglichen Zahlen $f(w)$ genau λ^r complexe Zahlen $f(u, u_1, u_2 \ldots)$, welche eben so viele Ambigen darstellen. Die Anzahl aller Ambigen, welche auf diese Weise erhalten werden, ist also gleich $\lambda^{\lambda-2+r}$, welche in so fern ebenfalls als ursprünglich angesehen werden können, als keine derselben aus einer andern durch Multiplikation mit einer wirklichen complexen Zahl in z erzeugt werden kann. Alle anderen Ambigen aber können aus diesen $\lambda^{\lambda-2+r}$ durch Multiplikation mit wirklichen complexen Zahlen in z erzeugt werden.

Aus den gefundenen Ambigen sollen nun die nichtäquivalenten ambigen Klassen ermittelt werden. Aus der Definition der Äquivalenz, nach welcher zwei ideale complexe Zahlen in z äquivalent sind, wenn sie durch Zusammensetzung mit einer und derselben dritten idealen Zahl zu wirklichen complexen Zahlen in z werden, folgt zunächst, daſs alle Ambigen, welche aus einer einzigen $f(u, u_1, u_2, \ldots)$ entstehen, indem diese mit wirklichen complexen Zahlen in z zusammengesetzt wird, nothwendig äquivalent sind; denn wenn $F(u, u_1, u_2 \ldots)$ ein in der Theorie der complexen Zahlen in z idealer Multiplikator ist, welcher mit $f(u, u_1, u_2 \ldots)$ zusammengesetzt, eine wirkliche complexe Zahl in z ergiebt, so ergiebt derselbe auch in seiner Zusammensetzung mit $f(u, u_1, u_2 \ldots)\, G(z)$ eine wirkliche complexe Zahl in z, wenn $G(z)$ wirklich ist. Die nichtäquivalenten Klassen der Ambigen sind aus diesem Grunde nur unter den $\lambda^{\lambda-2+r}$ aufzusuchen, welche sich nicht durch Multiplikation mit wirklichen complexen Zahlen in z aus einander erzeugen lassen.

Wenn nun $f(u, u_1, u_2 \ldots)$, als wirkliche complexe Zahl in der Theorie der aus den Wurzeln u, u_1, u_2 gebildeten complexen Zahlen, eine ideale Zahl in der Theorie der complexen Zahlen in z darstellt, und $E(u, u_1, u_2 \ldots)$ bezeichnet eine Einheit in $u, u_1, u_2 \ldots$, d. h. eine wirkliche complexe Zahl dieser Theorie, deren Norm eine Einheit in α ist, so muſs nothwendig $E(u, u_1, u_2 \ldots)\, f(u, u_1, u_2 \ldots)$ vollständig dieselbe ideale Zahl in z darstellen, als $f(u, u_1, u_2 \ldots)$, weil eine ideale Zahl in Beziehung auf Einheiten, mit denen sie behaftet sein kann, vollständig unbestimmt ist. Zu-

gleich ist klar, dafs $E(u, u_1, u_2 \ldots) f(u, u_1, u_2 \ldots)$ alle Darstellungen einer und derselben idealen Zahl als wirkliche complexe Zahl in $u, u_1, u_2 \ldots$ erschöpft, weil die durch ihre idealen Primfaktoren definirten, wirklichen complexen Zahlen sich lediglich durch Einheiten unterscheiden können. Wenn es sich aber, wie in dem vorliegenden Falle nur um solche Zahlen $f(u, u_1, u_2 \ldots)$ handelt, die einer Gleichung von der Form (4.) genügen, so mufs die Einheit $E(u, u_1, u_2 \ldots)$, mit welcher $f(u, u_1, u_2 \ldots)$ behaftet genommen werden kann, selbst einer Gleichung von derselben Form genügen. Diese Bedingung läfst sich so ausdrücken: der Quotient zweier conjugirten Einheiten $E(u\alpha, u_1, u_2 \ldots)$ und $E(u, u_1, u_2 \ldots)$ mufs einer wirklichen complexen Zahl in z gleich sein, der Quotient zweier Einheiten aber ist selbst wieder eine Einheit, es mufs also

$$(5.) \qquad \frac{E(u\alpha, u_1, u_2 \ldots)}{E(u, u_1, u_2 \ldots)} = E(z)$$

sein, wo $E(z)$ eine ganze Einheit in z ist. Eine Einheit $E(u, u_1, u_2 \ldots)$, welche dieser Bedingung genügt, soll in dem Folgenden eine ambige Einheit genannt werden.

Die Untersuchung, ob unter den $\lambda^{\lambda-2+r}$ Ambigen der Form $f(u, u_1, u_2 \ldots)$ noch äquivalente vorhanden sind, und die Zurückführung derselben auf das System der nichtäquivalenten wird nun in folgender Weise geleistet. Es seien $f(u, u_1, u_2 \ldots)$ und $f'(u, u_1, u_2 \ldots)$ zwei beliebige dieser $\lambda^{\lambda-2+r}$ Ambigen, so ist

$$(6.) \qquad \frac{Nf(u, u_1, u_2 \ldots)}{f(u, u_1, u_2 \ldots)} = F(u, u_1, u_2 \ldots)$$

eine ganze complexe Zahl in $u, u_1, u_2 \ldots$, welche mit $f(u, u_1, u_2 \ldots)$ multiplicirt ein in der Theorie der complexen Zahlen in z wirkliches Produkt giebt. Wenn nun $f(u, u_1, u_2 \ldots)$ mit $f'(u, u_1, u_2 \ldots)$ äquivalent sein soll, so mufs dieselbe Zahl $F(u, u_1, u_2 \ldots)$ auch mit der andern zusammengesetzt eine wirkliche complexe Zahl in z ergeben. Weil aber die Zahl $f'(u, u_1, u_2 \ldots)$, in so fern sie eine ideale Zahl in z darstellt, und in so fern sie einer Gleichung von der Form (4.) genügen soll, mit einer beliebigen ambigen Einheit $E(u, u_1, u_2 \ldots)$ multiplicirt genommen werden kann, so hat man

$$(7.) \qquad F(u, u_1, u_2 \ldots)\, E(u, u_1, u_2 \ldots)\, f'(u, u_1, u_2 \ldots) = G(z)$$

gleich einer ganzen complexen Zahl in z. Multiplicirt man diese Gleichung

mit $f(u, u_1, u_2 \ldots)$ und dividirt durch $G(z)$, so kann man diese Bedingung auch so aussprechen:

(I.) Alle Ambigen von der Form $f(u, u_1, u_2 \ldots)$, welche aus einer derselben entstehen, indem diese mit einer ambigen Einheit und mit einer wirklichen complexen Zahl in z multiplicirt wird, (welche letztere gebrochen sein kann, aber so, dafs sie in der Norm ihres Nenners weder ϱ noch die Faktoren von $D(\alpha)$ enthält), sind mit dieser Ambigen äquivalent, und umgekehrt: alle Ambigen, welche mit einer derselben äquivalent sind, lassen sich auf die angegebene Weise aus dieser einen ableiten.

Es seien jetzt $E(u, u_1, u_2 \ldots)$ und $E_1(u, u_1, u_2 \ldots)$ zwei verschiedene ambige Einheiten, von der Art, dafs die eine aus der anderen nicht durch Multiplikation mit einer Einheit $E(z)$ entstehen kann; es sei ferner $f(u, u_1, u_2 \ldots)$ eine Ambige, so sind

$$E(u, u_1, u_2 \ldots) f(u, u_1, u_2 \ldots) \text{ und } E_1(u, u_1, u_2 \ldots) f(u, u_1, u_2 \ldots)$$

zwei Ambigen, welche durch Multiplikation mit einer complexen Zahl in z nicht aufeinander zurückgeführt werden können, welche also dem Systeme der oben als ursprünglich bezeichneten $\lambda^{\lambda-2+r}$ Ambigen angehören, und dabei äquivalent sind. Es folgt hieraus, dafs eine jede Ambige in diesem Systeme der ursprünglichen Ambigen genau so viele äquivalente hat, als es ambige Einheiten giebt, die durch Multiplikation mit Einheiten in z auf einander nicht zurückgeführt werden können. Also wenn die Anzahl der in diesem Sinne von einander unabhängigen ambigen Einheiten mit E bezeichnet wird, so sind genau je E dieser $\lambda^{\lambda-2+r}$ Ambigen äquivalent, und die Anzahl aller nicht äquivalenten Ambigen ist darum gleich dem Eten Theile von $\lambda^{\lambda-2+r}$. Es folgt hieraus, dafs E eine Potenz von λ sein mufs, und dafs $E = \lambda^t$ gesetzt werden kann. Das gefundene Resultat giebt folgenden Satz:

(II.) Wenn die Anzahl der ambigen Einheiten, welche durch Multiplikation mit Einheiten in z sich nicht auf einander zurückführen lassen, gleich λ^t ist, und die Anzahl der in der Determinante $D(\alpha)$ enthaltenen verschiedenen Primfaktoren gleich r, so ist die Anzahl aller nicht äquivalenten Klassen der Ambigen gleich $\lambda^{\lambda-2+r-t}$.

§. 12.

Die complexen Einheiten in w und in z.

Zur vollständigen Bestimmung der Anzahl aller nichtäquivalenten, ambigen Klassen in der Theorie der complexen Zahlen in z, ist jetzt nur noch erforderlich, die Anzahl $E = \lambda^{\epsilon}$ der von einander unabhängigen ambigen Einheiten zu finden. Hierbei mache ich von den Resultaten Gebrauch, welche Hr. Dirichlet in seinen Untersuchungen über die, in der Theorie der allgemeinen, zerlegbaren Formen vorkommenden Einheiten gefunden, und im März 1846 der Königlichen Akademie mitgetheilt hat, m. s. den Monatsbericht.

Wenn eine irreduktible Gleichung des 2νten Grades, mit nichtcomplexen, ganzzahligen Coefficienten zu Grunde gelegt wird, deren Wurzeln alle imaginär sind, so giebt es nach Dirichlet in der Theorie der complexen Zahlen, welche rationale Funktionen einer Wurzel der gegebenen Gleichung, mit ganzzahligen Coefficienten sind, genau $\nu - 1$ complexe Einheiten, welche ein vollständiges, unabhängiges System von Einheiten dieser Theorie bilden. Ein System von Einheiten wird ein unabhängiges genannt, wenn ein Produkt von Potenzen dieser Einheiten nicht gleich Eins sein kann, ohne dafs die Exponenten der Potenzen alle einzeln gleich Null sind, und ein solches System von unabhängigen Einheiten ist zugleich ein vollständiges, wenn demselben keine Einheit weiter hinzugefügt werden kann, ohne dafs die Eigenschaft der Unabhängkeit des Systems dadurch verloren geht. Ein unabhängiges und vollständiges System hat die Eigenschaft, dafs alle complexen Einheiten dieser Theorie als Produkte von Potenzen der unabhängigen Einheiten sich darstellen lassen, wenn noch gewisse einfache Einheiten, welche nur Einheitswurzeln sind, als Faktoren hinzugenommen werden. Die Exponenten derjenigen Potenzen der unabhängigen Einheiten, durch deren Produkte alle Einheiten dargestellt werden können, haben niemals andere als rationale Zahlenwerthe. Ein unabhängiges und vollständiges System, durch welches alle Einheiten sich so darstellen lassen, dafs die Exponenten der Potenzen nur ganze Zahlen sind, heifst ein System von Fundamentaleinheiten.

Um nun diese allgemeinen Resultate auf die Untersuchung der Einheiten in w und in z anzuwenden, welche aufser den irrationalen Gröfsen w oder z auch noch die Wurzel α enthalten, mufs man eine irreduktible Gleichung mit nichtcomplexen, ganzzahligen Coefficienten aufstellen, von der Art, dafs durch eine Wurzel derselben, so wohl α, als auch w, und demgemäfs auch z, sich rational darstellen lasse. Ich wähle hierzu diejenige Gleichung, deren Wurzel $y = \alpha + w$ ist. Diese giebt zunächst

$$(1.) \qquad (y-\alpha)^\lambda - D(\alpha) = 0,$$

und demgemäfs, wenn für α seine $\lambda - 1$ Werthe α, α^2, ... $\alpha^{\lambda-1}$ gesetzt werden, und das Produkt gebildet wird:

$$(2.) \quad ((y-\alpha)^\lambda - D(\alpha))\,((y-\alpha^2)^\lambda - D(\alpha^2))\,\ldots\,((y-\alpha^{\lambda-1})^\lambda - D(\alpha^{\lambda-1})) = 0,$$

welche Gleichung vom Grade $\lambda(\lambda-1)$, vollständig entwickelt, nichtcomplexe ganze Zahlen zu Coefficienten hat. Dafs diese Gleichung irreduktibel ist, folgt daraus, dafs die $\lambda - 1$ Faktoren, aus denen sie zusammengesetzt ist, einzeln in dem Sinne irreduktibel sind, dafs sie nicht in Faktoren niederer Grade, deren Coefficienten rational in α wären, sich zerlegen lassen, wenn nämlich die Determinante $D(\alpha)$, wie überall vorausgesetzt wird, nicht eine vollständige λte Potenz ist. Ein jeder Faktor der Gleichung (2.), welcher nichtcomplexe rationale Zahlen als Coefficienten hätte, müsste darum nur ein Produkt einer Anzahl jener $\lambda - 1$ Faktoren des λten Grades sein. Entwickelt man aber ein solches Produkt nach Potenzen von y, so erkennt man schon aus der Betrachtung des Coefficienten des zweiten Gliedes, dafs dasselbe nicht anders rationale Coefficienten haben kann, als wenn es alle diese $\lambda - 1$ Faktoren der Gleichung (2.) umfasst.

Um nun α als rationale Funktion von y zu bestimmen, hat man nur die gemeinsame Wurzel α der beiden Gleichungen

$$(y-\alpha)^\lambda - D(\alpha) = 0 \text{ und } 1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$$

zu suchen. Diese Gleichungen haben nämlich nur die eine gemeinschaftliche Wurzel α; denn hätten sie aufserdem auch eine andere Wurzel α^k mit einander gemein, so müsste die Wurzel $y = \alpha + w$ der Wurzel $y = \alpha^k + \sqrt[\lambda]{D(\alpha^k)}$ gleich sein, und die Gleichung (2.) wäre nicht irreduktibel. Da also α eine rationale Funktion von y ist, so kann man demselben die Form

$$\alpha = \frac{f(y)}{\delta}$$

geben, wo δ ein von der Determinante $D(\alpha)$ abhängiger, nichtcomplexer ganzzahliger Nenner ist, und $f(y)$ eine ganze, rationale Funktion von y des Grades $\lambda(\lambda-1)-1$, mit ganzzahligen Coefficienten. Es ist alsdann $w = y - \alpha$ eine rationale Funktion derselben Art, mit demselben Nenner δ, und da demnach auch die Potenzen $\alpha, \alpha^2, \alpha^3, \ldots \alpha^{\lambda-1}$, so wie die Potenzen $w, w^2, w^3, \ldots w^{\lambda-1}$ sich als rationale Funktionen von y ausdrücken lassen, deren Nenner nur Potenzen von δ sind, so folgt, daſs jede ganze und ganzzahlige Funktion von α und w, d. i. jede complexe Zahl in w sich als gebrochene rationale Funktion von y darstellen läſst, deren Nenner eine bestimmte, nur von der Determinante $D(\alpha)$ abhängige, ganze nichtcomplexe Zahl Δ ist, daſs also

$$\Delta F(w, \alpha) = F(y) \tag{3.}$$

ist, wo $F(y)$, als ganze und ganzzahlige rationale Funktion von y, auch complexe Zahl in y genannt werden kann. Das Δfache einer jeden ganzen complexen Zahl in w läſst sich also als ganze complexe Zahl in y darstellen.

Eine ganze complexe Zahl in w enthält im Ganzen $\lambda(\lambda-1)$ Coefficienten, welche nichtcomplexe ganze Zahlen sind, wenn man alle ihre Glieder, welche verschiedene Potenzen von α und w enthalten, besonders betrachtet. In Beziehung auf einen gegebenen Modul Δ kann jeder dieser $\lambda(\lambda-1)$ Coefficienten die Δ verschiedenen Reste $0, 1, 2, \ldots \Delta-1$ geben, es giebt daher nach dem Modul Δ nicht mehr als $\Delta^{\lambda(\lambda-1)}$ incongruente complexe Zahlen in w. Erhebt man nun eine complexe Einheit in w: $E(w)$ zu Potenzen, so müssen in der Reihe

$$1, \quad E(w), \quad E(w)^2, \quad E(w)^3, \quad E(w)^4 \ldots\ldots$$

wenn dieselbe so weit fortgesetzt wird, daſs sie mehr als $\Delta^{\lambda(\lambda-1)}$ Glieder enthält, nothwendig nach dem Modul Δ congruente Glieder vorkommen, man hat also

$$E(w)^m \equiv E(w)^n, \quad \text{mod. } \Delta,$$

wo m und n verschiedene Zahlen sind und nicht gröſser als $\Delta^{\lambda(\lambda-1)}$. Es hat nun $E(w)$, als Einheit, keinen gemeinschaftlichen Faktor mit dem Modul Δ, man kann also, wenn $n < m$ ist, diese Congruenz durch $E(w)^n$ dividiren, und erhält so

$$E(w)^{n-s} \equiv 1, \text{ mod. } \Delta,$$

oder als Gleichung geschrieben:

$$(4.) \qquad E(w)^{n-s} = 1 + \Delta F(w),$$

und weil $\Delta F(w)$, wie oben gezeigt worden, eine ganze complexe Zahl in y ist, so erkennt man hieraus, dafs eine bestimmte Potenz einer jeden complexen Einheit in w sich als ganze complexe Einheit in y darstellen läfst.

Aus der Definition eines vollständigen Systems von Einheiten geht hervor, dafs dasselbe diese beiden Eigenschaften behält, wenn man die einzelnen Einheiten, aus welchen es besteht, zu irgend welchen ganzen Potenzen erhebt; wenn man daher die Einheiten eines vollständigen, unabhängigen Systems in w zu denjenigen Potenzen erhebt, welche diese zu ganzen complexen Einheiten in y machen, so mufs man ein unabhängiges und vollständiges System von Einheiten in y erhalten, und weil die Anzahl der Einheiten aus welchen dieses besteht, nach dem Dirichletschen Satze gleich $\frac{\lambda(\lambda-1)}{2} - 1$ ist, so mufs ein vollständiges, unabhängiges System von Einheiten in w nothwendig genau eben so viele Einheiten enthalten. Weil ferner die λte Potenz einer jeden complexen Zahl in w eine complexe Zahl in z, also auch die λte Potenz einer jeden Einheit in w eine Einheit in z ist, so folgt, dafs auch ein vollständiges unabhängiges System von Einheiten in z genau $\frac{\lambda(\lambda-1)}{2} - 1$ Einheiten enthalten mufs.

Die complexen Einheiten der niederen Theorie in α sind unter den Einheiten der höheren Theorie in w oder in z als besondere mit enthalten, die unabhängigen Einheiten dieser niederen Theorie können also auch mit als unabhängige Einheiten der höheren Theorie benutzt werden. Setzt man nun, wie im §. 6. der Kürze halben $\mu = \frac{\lambda-1}{2}$, $\nu = \frac{\lambda(\lambda-1)}{2}$, so hat man $\mu - 1$ unabhängige Einheiten in α, und da die Anzahl aller unabhängigen Einheiten in w oder in z gleich $\nu - 1$ ist, so hat man zu diesen $\mu - 1$ Einheiten in α noch $\nu - \mu$ Einheiten in w oder in z hinzuzunehmen, damit das System vollständig werde. Diese $\nu - \mu$ Einheiten der höheren Theorie kann man immer so wählen, dafs ihre Normen, welche nicht complexe Einheiten in α sind, gleich Eins selbst werden. Wenn nämlich eine Einheit $E(w)$ diese Bedingung nicht erfüllt, sondern die Norm $\varepsilon(\alpha)$ hat, so nehme man anstatt derselben ihre λte Potenz, dividirt durch $\varepsilon(\alpha)$, wobei weder die Vollständigkeit noch die Unabhängigkeit des Systems beeinträchtigt wird,

die an die Stelle von $E(w)$ tretende Einheit aber die verlangte Eigenschaft hat; wenn es sich um eine Einheit $E(z)$ handelt, so ist deren Norm schon von selbst eine λte Potenz, gleich $\varepsilon(\alpha)^{\lambda}$, man hat sie daher nur durch $\varepsilon(\alpha)$ zu dividiren. Also:

(I.) Es giebt genau $\nu - \mu = \frac{(\lambda-1)(\lambda-1)}{2}$ unabhängige complexe Einheiten in w oder in z, deren Normen gleich Eins sind.

Um die nun folgenden Sätze leichter beweisen und anschaulicher darstellen zu können, mache ich von einer eigenthümlichen Art der Bezeichnung Gebrauch, welche Hr. Kronecker in seiner Dissertation *de unitatibus complexis*. Berol. 1845. zuerst eingeführt hat, und welche in allen Fällen, wo man es mit Produkten von Potenzen conjugirter Einheiten zu thun hat, höchst vortheilhaft ist. Ich bezeichne, wie diefs Hr. Kronecker in einer ähnlichen Untersuchung gethan hat, ein Produkt von der Form

$$E(w)^{a}\, E(w\alpha)^{a_1}\, E(w\alpha^2)^{a_2} \ldots\ldots E(w\alpha^{\lambda-1})^{a_{\lambda-1}},$$

gleichsam als Potenz mit einem complexen Exponenten durch

$$E(w)^{a + a_1\alpha + a_2\alpha^2 + \ldots\ldots + a_{\lambda-1}\alpha^{\lambda-1}}$$

oder noch kürzer, wenn der Exponent als complexe Zahl in α mit $a(\alpha)$ bezeichnet wird:

$$(5.) \qquad E(w)^{a}\, E(w\alpha)^{a_1}\, E(w\alpha^2)^{a_2} \ldots\ldots E(w\alpha^{\lambda-1})^{a_{\lambda-1}} = E(w)^{a(\alpha)}.$$

Ebenso, wenn es sich um complexe Einheiten in z handelt, hat man

$$(6.) \qquad E(z)^{a}\, E(z_1)^{a_1}\, E(z_2)^{a_2} \ldots\ldots E(z_{\lambda-1})^{a_{\lambda-1}} = E(z)^{a(\alpha)}.$$

Wenn den Potenzen der Einheiten mit complexen Exponenten dieser bestimmte Sinn gegeben wird, so kann man den complexen Exponenten $a(\alpha)$ mit Hülfe der Gleichung $1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$ beliebig verändern, ohne dafs dieses Zeichen seinen Werth ändert, denn es ist

$$(7.) \quad E(w)^{1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1}} = E(w)\, E(w\alpha)\, E(w\alpha^2) \ldots E(w\alpha^{\lambda-1}) = 1.$$

Ferner findet für diese Potenzen mit complexen Exponenten genau dieselbe Regel der Multiplikation Statt, als für gewöhnliche Potenzen, denn man hat:

$$(8.) \qquad E(w)^{a(\alpha)}\, E(w)^{b(\alpha)} = E(w)^{a(\alpha) + b(\alpha)},$$

weil die eine, so wie die andere Seite nichts anderes darstellt, als das Produkt

$$E(w)^{a+b} \, E(w\alpha)^{a_1+b_1} \, E(w\alpha^2)^{a_2+b_2} \ldots . \, E(w\alpha^{\lambda-1})^{a_{\lambda-1}+b_{\lambda-1}} .$$

Ebenso findet für diese Potenzen mit complexen Exponenten auch dieselbe Regel der Potenzerhebung einer Potenz Statt, wie für gewöhnliche Potenzen, denn man hat die Regel:

$$(9.) \qquad \left(E(w)^{a(\alpha)}\right)^{b(\alpha)} = E(w)^{a(\alpha)b(\alpha)},$$

von deren Richtigkeit man sich sogleich überzeugen kann, wenn man auf beiden Seiten dieser Gleichung die Potenzen der Einheit mit complexen Exponenten als Produkte von Potenzen der conjugirten Einheiten darstellt.

Mit Hülfe solcher Potenzen von Einheiten mit complexen Exponenten will ich nun zeigen, wie ein vollständiges System der $\nu - \mu$ unabhängigen Einheiten in w oder in z, deren Normen gleich Eins sind, durch μ verschiedene Einheiten dieser Art, mit ihren conjugirten dargestellt werden kann.

Wenn $E(w)$ irgend eine Einheit ist, deren Norm gleich Eins ist, so zeige ich zunächst, dafs die $\lambda - 1$ conjugirten Einheiten

$$E(w), \; E(w\alpha), \; E(w\alpha^2), \; \ldots \; E(w\alpha^{\lambda-2})$$

von einander unabhängig sind, dafs also die Gleichung

$$(10.) \qquad E(w)^{m} \, E(w\alpha)^{m_1} \, E(w\alpha^2)^{m_2} \ldots E(w\alpha^{\lambda-2})^{m_{\lambda-2}} = 1,$$

in welcher die Exponenten $m, m_1, m_2, \ldots m_{\lambda-2}$ rationale, oder was hier dasselbe ist, ganze Zahlen sind, nicht bestehen kann, ohne dafs sie alle den Werth Null erhalten. Setzt man

$$m + m_1\alpha + m_2\alpha^2 + \ldots . + m_{\lambda-2}\alpha^{\lambda-2} = m(\alpha),$$

und erhebt beide Seiten der Gleichung

$$E(w)^{m(\alpha)} = 1$$

zur Potenz $M(\alpha)$, wo $M(\alpha)$ durch die Gleichung $M(\alpha)\,m(\alpha) = Nm(\alpha)$ bestimmt ist, so erhält man

$$(11.) \qquad E(w)^{Nm(\alpha)} = 1.$$

Der Exponent Norm von $m(\alpha)$, ist eine nichtcomplexe Zahl, diese Potenz ist also eine Potenz im gewöhnlichen Sinne, welche, wenn $E(w)$ nicht eine einfache Wurzel der Einheit ist, nicht gleich Eins sein kann, ohne dafs $Nm(\alpha) = 0$ ist, also $m(\alpha) = 0$ und folglich $m = 0$, $m_1 = 0$, ... $m_{\lambda-2} = 0$, wegen der Irreduktibilität der Gleichung $1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$. Die $\lambda - 1$ conjugirten Einheiten

$$E(w),\ E(w\alpha),\ E(w\alpha^2)\ \ldots.,\ E(w\alpha^{\lambda-2})$$

bilden also in der That ein unabhängiges, aber unvollständiges System. Es sei nun $E_1(w)$ eine andere Einheit, deren Norm gleich Eins ist, welche mit dieser zusammen ein unabhängiges System bilde, so behaupte ich, dafs die conjugirten $\lambda - 1$ Einheiten

$$E_1(w),\ E_1(w\alpha),\ E_1(w\alpha^2)\ \ldots.\ E_1(w\alpha^{\lambda-2})$$

mit den obigen zusammen ein unabhängiges System von $2(\lambda - 1)$ Einheiten bilden, dafs also die Gleichung

$$(12.)\qquad E(w)^{m(\alpha)}\, E_1(w)^{m_1(\alpha)} = 1$$

nicht bestehen kann, ohne dafs die complexen Exponenten $m(\alpha)$ und $m_1(\alpha)$ beide gleich Null sind. Erhebt man nämlich diese Gleichung zur Potenz $M_1(\alpha)$, wo $M_1(\alpha)$ durch die Gleichung $M_1(\alpha)\, m_1(\alpha) = Nm_1(\alpha)$ bestimmt ist, so hat man

$$(13.)\qquad E(w)^{M_1(\alpha)m(\alpha)}\, E_1(w)^{Nm_1(\alpha)} = 1,$$

welches, da $Nm_1(\alpha)$ eine nichtcomplexe Zahl ist, und darum $E_1(w)^{Nm_1(\alpha)}$ eine Potenz im gewöhnlichen Sinne des Wortes, der Voraussetzung widerspricht, nach welcher $E_1(w)$ eine Einheit ist, die mit den $\lambda - 1$ zu $E(w)$ conjugirten ein unabhängiges System bildet. Wenn nun $E_2(w)$ eine andere Einheit mit der Norm Eins ist, welche mit den bereits aufgestellten $2(\lambda - 1)$ Einheiten zusammen ein unabhängiges System bildet, so wird ganz auf dieselbe Weise bewiesen, dafs auch die conjugirten $\lambda - 1$ Einheiten

$$E_2(w),\ E_2(w\alpha),\ E_2(w\alpha^2),\ \ldots.\ E_2(w\alpha^{\lambda-2})$$

mit jenen $2(\lambda - 1)$ Einheiten zusammen ein unabhängiges System von $3(\lambda - 1)$ Einheiten bilden. Auf diese Weise kann man nun fortfahren, bis man ein vollständiges unabhängiges System von Einheiten, deren Normen gleich

Eins sind, erlangt hat, welches, wie oben gezeigt worden ist, aus $\nu-\mu$ Einheiten besteht. Da $\nu-\mu=\frac{\lambda(\lambda-1)}{2}-\frac{\lambda-1}{2}=\mu(\lambda-1)$ ist, so folgt, dafs die Anzahl der Einheiten, welche mit ihren conjugirten zusammen ein vollständiges System bilden, gleich μ ist. Was hier von den Einheiten in w bewiesen ist, gilt nothwendig auch von den Einheiten der specielleren Theorie in z, man hat also folgenden Satz:

(II.) Es giebt genau μ Einheiten in w oder in z, welche, wenn man von einer jeden derselben $\lambda-1$ conjugirte nimmt, ein vollständiges unabhängiges System von $\mu(\lambda-1)$ Einheiten bilden, deren Normen gleich Eins sind.

Wenn nun die μ Einheiten:

$$E(w),\ E_1(w),\ E_2(w),\ \ldots.\ E_{\mu-1}(w)$$

mit ihren conjugirten ein vollständiges und unabhängiges System aller derjenigen Einheiten bilden, deren Normen gleich Eins sind, so kann aus diesem Systeme stets ein anderes hergestellt werden, dessen μ Einheiten

$$\varepsilon(w),\ \varepsilon_1(w),\ \varepsilon_2(w),\ \ldots.\ \varepsilon_{\mu-1}(w)$$

so beschaffen sind, dafs keine in der Form

$$\varepsilon(w)^{M}\ \varepsilon_1(w)^{M_1}\ \varepsilon_2(w)^{M_2}\ \ldots.\ \varepsilon_{\mu-1}(w)^{M_{\mu-1}}$$

enthaltene Einheit eine ϱte Potenz einer Einheit sein kann, ohne dafs die ganzen complexen Exponenten M, M_1, M_2 ... $M_{\mu-1}$ alle einzeln durch ϱ theilbar sind. Ein so beschaffenes System kann ein beziehungsweise fundamentales genannt werden, nämlich fundamental in Beziehung auf den Exponenten ϱ. Dasselbe wird aus dem gegebenen Systeme der Einheiten $E(w)$, $E_1(w)$ ... $E_{\mu-1}(w)$ auf folgende Weise hergeleitet.

Durch das gegebene System der Einheiten möge sich eine ϱ^k te Potenz einer Einheit so darstellen lassen, dafs die complexen Exponenten nicht alle durch ϱ theilbar sind, aber eine ϱ^{k+1}te Potenz einer Einheit soll nicht mehr in dieser Weise durch dieses System darstellbar sein, so hat man

$$(14.)\qquad E(w)^{A}\ E_1(w)^{A_1}\ E_2(w)^{A_2}\ \ldots.\ E_{\mu-1}(w)^{A_{\mu-1}}=\varepsilon(w)^{\varrho^k}$$

für bestimmte Werthe der complexen Exponenten A, A_1, ... $A_{\mu-1}$, und weil wenigstens einer derselben durch ϱ nicht theilbar ist, so kann man den ersten A als einen solchen wählen. Durch die $\mu-1$ Einheiten $E_1(w)$,

$E_2(w)$, ... $E_{\mu-1}(w)$, mit Ausschlufs von $E(w)$, lasse sich eine ϱ^{k_1}te, aber nicht eine ϱ^{k_1+1}te Potenz einer Einheit so darstellen, dafs nicht alle complexen Exponenten dieser Einheiten durch ϱ theilbar sind, so hat man

$$(15.)\qquad E_1(w)^{B_1}\,E_2(w)^{B_2}\,\ldots.\,E_{\mu-1}(w)^{B_{\mu-1}} = \varepsilon_1(w)^{\varrho^{k_1}},$$

und man kann hier ebenfalls den ersten Exponenten B_1 als einen der durch ϱ nicht theilbaren nehmen. Ebenso sei durch diese Einheiten, wenn weiter die Einheit $E_1(w)$ ausgeschlossen wird, noch eine ϱ^{k_2}te Potenz, aber nicht eine ϱ^{k_2+1}te Potenz einer Einheit darstellbar, so hat man

$$(16.)\qquad E_2(w)^{C_2}\,E_3(w)^{C_3}\,\ldots.\,E_{\mu-1}(w)^{C_{\mu-1}} = \varepsilon_2(w)^{\varrho^{k_2}}.$$

wo wieder C_2 als einer der nicht durch ϱ theilbaren Exponenten genommen werden kann. So fortfahrend erhält man die μ Einheiten $\varepsilon(w)$, $\varepsilon_1(w)$, ... $\varepsilon_{\mu-1}(w)$, von denen nun bewiesen werden soll, dafs sie ein System bilden, welches die verlangte Eigenschaft besitzt.

Gesetzt es wäre für irgend welche bestimmte ganze complexe Exponenten M, M_1, ... $M_{\mu-1}$, die nicht alle durch ϱ theilbar sind,

$$(17.)\qquad \varepsilon(w)^{M}\,\varepsilon_1(w)^{M_1}\,\ldots.\,\varepsilon_{\mu-1}(w)^{M_{\mu-1}} = e(w)^{\varrho},$$

und M_r der erste, nicht durch ϱ theilbare Exponent, so hätte man auch

$$(18.)\qquad \varepsilon_r(w)^{M_r}\,\varepsilon_{r+1}(w)^{M_{r+1}}\,\ldots\,\varepsilon_{\mu-1}(w)^{M_{\mu-1}} = e_1(w)^{\varrho}.$$

Wenn nun zur ϱ^{k_r}ten Potenz erhoben wird, so kann man, weil von den Zahlen k, k_1, k_2 ... keine folgende gröfser sein kann, als die vorhergehende, die in diesem Ausdrucke vorkommenden ϱ^{k_r}ten Potenzen der Einheiten $\varepsilon_r(w)$, $\varepsilon_{r+1}(w)$, ... $\varepsilon_{\mu-1}(w)$ alle durch die Einheiten $E_r(w)$, $E_{r+1}(w)$ .... $E_{\mu-1}(w)$ ausdrücken, und erhält so einen Ausdruck von folgender Form:

$$(19.)\qquad E_r(w)^{K_r}\,E_{r+1}(w)^{K_{r+1}}\,\ldots.\,E_{\mu-1}(w)^{K_{\mu-1}} = e_1(w)^{\varrho^{k_r+1}},$$

in welchem der complexe Exponent K_r der ersten Einheit gleich dem Produkte des Exponenten M_r und des Exponenten H_r in dem Ausdrucke

$$(20.)\qquad E_r(w)^{H_r}\,E_{r+1}(w)^{H_{r+1}}\,\ldots.\,E_{\mu-1}(w)^{H_{\mu-1}} = \varepsilon_r(w)^{\varrho^{k_r}}$$

ist, und weil M_r und H_r nach der Voraussetzung nicht durch ϱ theilbar sind, so ist $K_r = M_r H_r$ ebenfalls nicht durch ϱ theilbar. Es ist aber nach der Voraussetzung unmöglich, eine ϱ^{k_r+1}te Potenz einer Einheit durch die Form (19.) auszudrücken, ohne dafs alle complexen Exponenten K_r, K_{r+1}, ... $K_{\mu-1}$ durch ϱ theilbar sind, also ist es auch unmöglich, durch die Einheiten $\varepsilon(w)$, $\varepsilon_1(w)$ ... $\varepsilon_{\mu-1}(w)$ eine ϱte Potenz irgend einer Einheit in dieser Weise auszudrücken. Genau dieselben Schlüsse gelten auch, wenn man anstatt der Einheiten in w die specielleren Einheiten in z zu Grunde legt, man hat also folgenden Satz:

(III.) Es giebt für Einheiten in w (oder in z), deren Normen gleich Eins sind, ein vollständiges und unabhängiges System von μ Einheiten mit ihren conjugirten, welches so beschaffen ist, dafs ein Produkt von Potenzen dieser μ Einheiten mit ganzen complexen Exponenten nicht eine ϱte Potenz einer Einheit in w (oder in z) darstellen kann, ohne dafs die complexen Exponenten der Potenzen aus denen dieses Produkt besteht, alle einzeln durch ϱ theilbar sind.

Weil das System der μ Einheiten $\varepsilon(w)$, $\varepsilon_1(w)$, ... $\varepsilon_{\mu-1}(w)$ mit ihren conjugirten ein vollständiges unabhängiges System für alle Einheiten ist, deren Normen gleich Eins sind, so kann man durch dasselbe alle Einheiten, deren Normen gleich Eins sind, darstellen, wenn man in den Coefficienten der complexen Exponenten M, M_1, ... $M_{\mu-1}$ der Form

$$(21.) \qquad \varepsilon(w)^{M}\ \varepsilon_1(w)^{M_1} \ \ldots\ \varepsilon_{\mu-1}(w)^{M_{\mu-1}}$$

rationale Brüche zuläfst, oder was dasselbe ist, wenn man diese Exponenten als gebrochene complexe Zahlen in α passend bestimmt. Diese gebrochenen Exponenten können nun, vermöge der in dem Satze (III.) ausgesprochenen Eigenthümlichkeit des vorliegenden Systems der unabhängigen Einheiten, in ihren Nennern niemals den Faktor ϱ enthalten, wenn gemeinschaftliche Faktoren der Zähler und Nenner nicht Statt haben, aus welchem Grunde ein solches System oben als ein in Beziehung auf ϱ fundamentales bezeichnet worden ist. Gesetzt es wäre eine ganze complexe Einheit $e(w)$ durch die Form (21.) so darstellbar, dafs irgend welche der gebrochenen complexen Exponenten M, M_1, ... $M_{\mu-1}$ in ihren Nennern ϱ enthielten, aber nicht in ihren Zählern, und es wäre ϱ^h die höchste Potenz von ϱ, welche

in einem dieser Nenner vorkommt, so würde der kleinste gemeinschaftliche Nenner, den man allen diesen gebrochenen Exponenten geben könnte, von der Form $\varrho^h N$ sein, wo N eine nicht weiter durch ϱ theilbare complexe Zahl in α wäre. Wenn man also eine durch die Form (21.) ausgedrückte Einheit zur $\varrho^h N$ten Potenz erhöbe, so würde man die Potenz, welche eine ϱte Potenz einer Einheit ist, durch dieselbe Form (21.) aber mit ganzen complexen Exponenten, welche alle nicht durch ϱ theilbar sind, ausgedrückt erhalten. Da dieses nicht möglich ist, so folgt, daſs die gebrochenen Exponenten M, M_1, ... $M_{\mu-1}$ in ihren Nennern niemals den Faktor ϱ enthalten können.

Wegen dieser Eigenschaft der Exponenten M, M_1, ... $M_{\mu-1}$ kann man von denselben die kleinsten nicht negativen, ganzen, nichtcomplexen Zahlen absondern, denen sie congruent sind nach dem Modul ϱ, und erhält so:

(22.) $M = a + \varrho M'$, $M_1 = a_1 + \varrho M'_1$, ... $M_{\mu-1} = a_{\mu-1} + \varrho M'_{\mu-1}$,

wo die Zahlen a, a_1, ... $a_{\mu-1}$ nur die Werthe 0, 1, 2, ... $\lambda - 1$ haben können. Die Form (21.) giebt demnach folgende Form:

$$(23.)\quad \varepsilon(w)^{a}\,\varepsilon_1(w)^{a_1} \ldots \varepsilon_{\mu-1}(w)^{a_{\mu-1}} \left(\varepsilon(w)^{M'}\,\varepsilon_1(w)^{M'_1} \ldots \varepsilon_{\mu-1}(w)^{M'_{\mu-1}}\right)^{\varrho},$$

welche ebenfalls alle Einheiten darstellt, deren Normen gleich Eins sind. Also alle Einheiten, deren Normen gleich Eins sind, entstehen aus den in der Form

$$(24.)\quad \varepsilon(w)^{a}\,\varepsilon_1(w)^{a_1} \ldots\ldots \varepsilon_{\mu-1}(w)^{a_{\mu-1}}$$

enthaltenen, in welcher a, a_1, $a_{\mu-1}$ nur alle Werthe 0, 1, 2, ... $\lambda - 1$ haben, wenn diese mit ϱten Potenzen von Einheiten multiplicirt werden. Von zwei verschiedenen, in dieser Form (24.) enthaltenen Einheiten kann aber niemals eine aus der andern durch Multiplikation mit einer ϱten Potenz einer Einheit erzeugt werden; denn hätte man

$$\varepsilon(w)^{a}\,\varepsilon_1(w)^{a_1} \ldots \varepsilon_{\mu-1}(w)^{a_{\mu-1}} = \varepsilon(w)^{b}\,\varepsilon_1(w)^{b_1} \ldots \varepsilon_{\mu-1}(w)^{b_{\mu-1}}\; E(w)^{\varrho},$$

so wäre auch

$$(25.)\quad \varepsilon(w)^{a-b}\,\varepsilon_1(w)^{a_1-b_1} \ldots\ldots \varepsilon_{\mu-1}(w)^{a_{\mu-1}-b_{\mu-1}} = E(w)^{\varrho},$$

und weil durch diese Form keine ϱte Potenz einer Einheit ausgedrückt wer-

den kann, ohne dafs alle Exponenten einzeln durch ϱ theilbar sind, so müssen $a-b$, a_1-b_1, ... $a_{\mu-1}-b_{\mu-1}$ alle durch ϱ, und weil es nichtcomplexe ganze Zahlen sind, alle durch λ theilbar sein, welches nur dann möglich ist, wenn $a=b$, $a_1=b_1$ ... $a_{\mu-1}=b_{\mu-1}$, also nur dann, wenn die beiden in der Form (24.) enthaltenen Einheiten dieselben sind. Da die Anzahl aller verschiedenen in dieser Form enthaltenen Einheiten gleich λ^μ ist, indem jeder der μ Exponenten a, a_1, ... $a_{\mu-1}$ alle λ Werthe 0, 1, 2, ... $\lambda-1$ annehmen kann, so hat man folgenden Satz:

(IV.) Es giebt genau λ^μ complexe Einheiten in w (oder in z), deren Normen gleich Eins sind, von denen keine aus der andern durch Multiplikation mit einer ϱten Potenz einer Einheit abgeleitet werden kann, welche alle als Produkte von Potenzen von μ, in Beziehung auf ϱ, fundamentalen Einheiten so dargestellt werden können, dafs den Potenzexponenten alle Werthe 0, 1, 2, ... $\lambda-1$ gegeben werden.

§. 13.

Die ambigen Einheiten und die nichtäquivalenten Ambigen. Schlufs auf die Anzahl der wirklich vorhandenen Gattungen.

Aus den Einheiten in z, deren Normen gleich Eins sind, werden nun die ambigen Einheiten in folgender Weise hergeleitet. Wenn $E(z)$ eine solche Einheit ist, so bilde man den Ausdruck:

$$PE(z) = 1 + E(z) + E(z)\,E(z_1) \,\ldots.\, E(z)\,E(z_1) \ldots E(z_{\lambda-2}),$$

welcher als ganze complexe Zahl in z einfach durch $F(z)$ bezeichnet werden soll. Vermöge der Grundeigenschaft des Ausdrucks $PE(z)$, nach welcher

$$E(z)\,PE(z_1) = PE(z)$$

ist, hat man

$$E(z)\,F(z_1) = F(z). \tag{1.}$$

Die Zahl $F(z)$, welche einer solchen Gleichung genügt, hat aber, wie im §. 8. gezeigt worden ist, die Eigenschaft, dafs ihre $h$te Potenz, wenn h die Klassenanzahl der idealen Zahlen in a bezeichnet, sich in zwei Faktoren

$$F(z)^h = C \cdot \Delta(z) \tag{2.}$$

zerlegen läfst, deren einer, C, eine wirkliche, ganze complexe Zahl in α ist, der andere, $\Delta(z)$, eine wirkliche complexe Zahl in z, deren Norm keinen anderen Primfaktor enthält, als die, welche in $\varrho D(\alpha)$ vorkommen. Diese Zahl $\Delta(z)$ genügt vermöge der Gleichungen (1.) und (2.) der Gleichung:

$$(3.) \qquad E(z)^1\, \Delta(z_1) = \Delta(z).$$

Es ist nun oben im §. 9. gezeigt worden, dafs eine jede Zahl $f(z)$, welche einer Gleichung von der Form

$$L(\alpha) f(z_1) = M(z) f(z)$$

genügt, wenn sie zuerst als complexe Zahl in w dargestellt, und sodann $w = u\, u_1\, u_2 \ldots$ gesetzt wird, folgende Form annimmt:

$$(4.) \qquad f(z) = \varrho^{\nu}\, u^{n}\, u_1^{n_1}\, u_2^{n_2} \ldots f(u, u_1, u_2 \ldots),$$

in welcher die Norm von $f(u, u_1, u_2 \ldots)$ keinen Faktor mit $\varrho D(\alpha)$ gemein hat. Wendet man dieses Resultat auf die Zahl $\Delta(z)$ an, welche einer Gleichung derselben Form genügt, nämlich für $M(z) = E(z)^{-1}$ und $L(\alpha) = 1$, und beachtet, dafs die Norm von $\Delta(z)$ keinen anderen Primfaktor enthält, als ϱ und die Primfaktoren der Determinante $D(\alpha)$, so hat man

$$(5.) \qquad \Delta(z) = \varrho^{\nu}\, u^{n}\, u_1^{n_1}\, u_2^{n_2} \ldots E(u, u_1, u_2 \ldots)$$

wo $E(u, u_1, u_2 \ldots)$ eine Einheit ist, weil ihre Norm weder die in $\varrho D(\alpha)$ enthaltenen, noch auch die in $\varrho D(\alpha)$ nicht enthaltenen Primfaktoren haben darf. Verwandelt man ferner u in $u\alpha$, wodurch z in z_1 übergeht, so hat man

$$(6.) \qquad \Delta(z_1) = \varrho^{\nu}\, \alpha^{n}\, u^{n}\, u_1^{n_1}\, u_2^{n_2} \ldots E(u\alpha, u_1, u_2 \ldots),$$

also vermöge der Gleichung (3.)

$$(7.) \qquad \frac{E(u\alpha, u_1, u_2 \ldots)}{E(u, u_1, u_2 \ldots)} = \alpha^{-n}\, E(z)^{-1}$$

Die Einheit $E(u, u_1, u_2 \ldots)$ ist also **eine ambige Einheit**. Auf dieselbe Weise läfst sich aus jeder Einheit in z, deren Norm gleich Eins ist, eine ambige Einheit erzeugen.

Es ist nun weiter zu untersuchen, unter welchen Bedingungen zwei verschiedene Einheiten $E(z)$ und $E_1(z)$ zwei in der Art verschiedene ambige Einheiten erzeugen, dafs die eine aus der andern durch Multiplikation mit

einer Einheit in z nicht hergeleitet werden kann. Aus den beiden Einheiten $E(z)$ und $E_1(z)$ erhalte man die Ambigen $E(u, u_1, u_2 \ldots)$ und $E_1(u, u_1, u_2 \ldots)$, so ist

$$(8.) \qquad \frac{E(u\alpha, u_1, u_2 \ldots)}{E(u, u_1, u_2 \ldots)} = \alpha^{-n}\, E(z)^{-h},$$

$$(9.) \qquad \frac{E_1(u\alpha, u_1, u_2 \ldots)}{E_1(u, u_1, u_2 \ldots)} = \alpha^{-n_1}\, E_1(z)^{-h}.$$

Wenn nun die beiden ambigen Einheiten so beschaffen sind, dafs

$$(10.) \qquad E_1(u, u_1, u_2 \ldots) = E(u, u_1, u_2 \ldots)\, e(z),$$

so erhält man aus den beiden vorhergehenden Gleichungen

$$(11.) \qquad E_1(z)^h = \alpha^{n-n_1}\, E(z)^h\, e(z)^\varrho.$$

Da h nicht durch λ theilbar ist, so kann man zwei ganze Zahlen b und c so bestimmen, dafs sie der Gleichung $bh = 1 + c\lambda$ genügen, erhebt man daher die Gleichung (11.) zur $b$ten Potenz und nimmt $bh = 1 + c\lambda$, so erhält man

$$(12.) \qquad E_1(z) = E(z)\,\alpha^{(n-n_1)b}\, E_1(z)^{-c\lambda}\, E(z)^{c\lambda}\, e(z)^{b\varrho},$$

und weil eine λte Potenz einer Einheit zugleich als eine ϱte Potenz angesehen werden kann, so folgt, dafs abgesehen von einer Potenz von α, welche zu jeder Einheit $E(z)$ beliebig hinzugenommen werden kann, die Einheit $E_1(z)$ aus der Einheit $E(z)$ entsteht, indem diese mit einer ϱten Potenz einer Einheit multiplicirt wird. Umgekehrt, wenn

$$(13.) \qquad E_1(z) = \alpha^k\, e(z)^\varrho\, E(z)$$

ist, so erhält man aus den beiden Gleichungen (8.) und (9.):

$$(14.) \qquad \frac{E_1(u\alpha, u_1, u_2 \ldots)}{E_1(u, u_1, u_2 \ldots)} = \alpha^{n-n_1-hk}\, \frac{E(u\alpha, u_1, u_2 \ldots)\, e(z_1)^h}{E(u, u_1, u_2 \ldots)\, e(z)^h},$$

setzt man also

$$(15.) \qquad \frac{E_1(u, u_1, u_2 \ldots)}{E(u, u_1, u_2 \ldots)\, e(z)^h} = \varepsilon(u, u_1, u_2 \ldots),$$

so hat man

$$(16.) \qquad \varepsilon(u\alpha, u_1, u_2 \ldots) = \alpha^{-n+n_1+hk}\, \varepsilon(u, u_1, u_2 \ldots).$$

Muliplicirt man nun mit einem passend gewählten Produkte von der Form $u^m u_1^{m_1} u_2^{m_2} \ldots$, um die complexe Einheit $\varepsilon(u, u_1, u_2 \ldots)$ in eine complexe Zahl in w zu verwandeln und setzt

(17.) $$u^m u_1^{m_1} u_2^{m_2} \ldots \varepsilon(u, u_1, u_2 \ldots) = f(w),$$

so giebt die Gleichung (16.) eine Gleichung von der Form:

(18.) $$f(w\alpha) = \alpha^{\prime} f(w),$$

aus welcher folgt, daſs $f(w)$ nur eine Potenz von w sein kann, multiplicirt mit einer complexen Zahl in α. Man hat daher

$$u^m u_1^{m_1}, u_2^{m_2} \ldots \varepsilon(u, u_1, u_2 \ldots) = Cw^{s}$$

und wenn für w der Werth $u\, u_1\, u_2 \ldots$ gesetzt wird:

(19.) $$\varepsilon(u, u_1, u_2 \ldots) = Cu^{s-m} u_1^{s-m_1} u_2^{s-m_2} \ldots,$$

da aber $\varepsilon(u, u_1, u_2 \ldots)$ eine Einheit ist, und darum keinen Faktor $u, u_1, u_2 \ldots$ enthalten kann, so folgt, daſs $m = s$, $m_1 = s$, $m_2 = s \ldots$ sein muſs, und C eine complexe Einheit in α, also

(20.) $$\varepsilon(u, u_1, u_2 \ldots) = E(\alpha),$$

und folglich

(21.) $$E_1(u, u_1, u_2 \ldots) = E(u, u_1, u_2 \ldots)\, E(\alpha)\, e(z)^h$$

Die eine dieser ambigen Einheiten entsteht also aus der andern durch Multiplikation mit einer Einheit in z. Das gefundene Resultat giebt den Satz:

(I.) Alle ambigen Einheiten, welche durch Multiplikation mit Einheiten in z sich nicht auf einander zurückführen lassen, und nur diese, entstehen aus allen denjenigen Einheiten in z, mit der Norm gleich Eins, welche sich durch Multplikation mit ϱten Potenzen von Einheiten in z nicht auf einander zurückführen lassen.

Nach dem Satze (IV.) §. 12. ist die Anzahl derjenigen Einheiten in z mit der Norm Eins, welche durch Multiplikation mit ϱten Potenzen von Einheiten in z sich nicht auf einander zurückführen lassen, gleich λ^{μ}; daher ergiebt der gefundene Satz zugleich den folgenden:

N 2

(II.) **Die Anzahl aller ambigen Einheiten, welche durch Multiplikation mit Einheiten in z sich nicht auf einander zurückführen lassen, ist gleich λ^μ.**

Im §. 11. ist diese Anzahl der ambigen Einheiten mit $E = \lambda^\varepsilon$ bezeichnet worden, man hat also $\varepsilon = \mu = \frac{\lambda-1}{2}$, $\lambda - 2 + r - \varepsilon = \mu + r - 1$, und demnach ergiebt der Satz (II.) §. 11. den folgenden:

(III.) Wenn die Anzahl der in der Determinante $D(\alpha)$ enthaltenen verschiedenen Primfaktoren gleich r ist, so ist die Anzahl aller wesentlich verschiedenen, nicht äquivalenten Klassen der Ambigen gleich $\lambda^{\mu+r-1}$.

In Betreff der wirklich vorhandenen Gattungen der verschiedenen Klassen der idealen Zahlen in z giebt daher der Satz (V.) §. 7:

(IV.) Die Anzahl der wirklich vorhandenen Gattungen der idealen Klassen in der Theorie der complexen Zahlen in z ist nicht gröfser als $\lambda^{\mu+r-1}$.

Da die Anzahl der verschiedenen Charaktere der idealen Zahlen in z gleich $\mu + r$ ist, und mithin die Anzahl aller Gesamtcharaktere, oder die Anzahl aller angebbaren Gattungen gleich $\lambda^{\mu+r}$ ist, so kann man diesen Satz auch so aussprechen:

(V.) Die Anzahl der wirklich vorhandenen Gattungen ist nicht gröfser als der λte Theil aller blofs angebbaren Gattungen oder Gesamtcharaktere.

§. 14.

Congruenzbedingung für die Darstellbarkeit einer complexen Zahl in α als Norm einer wirklichen complexen Zahl in w.

Für die Anwendung dieser Theorie der complexen Zahlen auf den Beweis der allgemeinen Reciprocitätsgesetze reicht das gefundene Resultat über die Anzahl der Gattungen: dafs die Anzahl der wirklich vorhandenen nicht gröfser ist, als der λ'te Theil der angebbaren Gesamtcharaktere, nicht aus, es ist zu diesem Zwecke erforderlich auf die Frage: ob der λte Theil der angebbaren Gesamtcharaktere auch wirklich vorhandene Gattungen giebt, näher einzugehen und dieselbe wenigstens in gewissen besonderen Fällen

vollständig zu lösen. Ein Mittel hierzu gewähren die complexen Zahlen in w und die complexen Zahlen in u, u_1, u_2 ... Da nämlich die wirklichen complexen Zahlen in diesen Theorieen sich als ideale Zahlen in der Theorie der complexen Zahlen in z darstellen, so kann man untersuchen, in wie weit es gelingt, durch diese die $\lambda^{\mu+\nu-1}$ Gattungen, welche nach dem gefundenen Satze Statt haben können, auszufüllen, d. h. in wie weit man für jeden von den $\lambda^{\mu+\nu-1}$ Gesamtcharakteren eine entsprechende wirkliche complexe Zahl in w oder in u, u_1, u_2 ... finden kann. Die Grundlage dieser Untersuchung bildet eine Congruenz unter den Charakteren C_3, C_5, ... $C_{\lambda-1}$ einer jeden idealen Zahl in z, welche als wirkliche complexe Zahl in w dargestellt werden kann, welche darum jetzt hergeleitet werden soll.

Zunächst ist es hierzu nöthig den Charakter

$$C_{\lambda-1} = \frac{NF(\alpha) - 1}{\lambda}$$

in ähnlicher Weise wie die anderen ebenfalls durch Differenzialquotienten eines Logarithmus auszudrücken, welches vermittelst einer allgemeineren Formel geschehen kann, die folgendermaafsen gefunden wird: Man nehme eine ganze rationale Funktion der Variabeln x, $\phi(x)$, vom $\lambda - 1$ten Grade, deren Coefficienten beliebige Constanten sein können, und bilde das Produkt von λ Faktoren

$$(1.)\qquad \prod_{0}^{\lambda-1}{}_{r}\ \phi(x + k(\alpha^r - 1)) = \Phi(x, k).$$

Dasselbe ist, als Funktion von k betrachtet, eine ganze rationale Funktion vom Grade $\lambda(\lambda - 1)$, welche die Eigenschaft hat, dafs alle Glieder, welche k^λ und die höheren Potenzen von k enthalten, Vielfache von λ^2 sind, wovon man sich leicht überzeugt, wenn man bemerkt, dafs mit jedem einfachen k ein Faktor $\alpha^r - 1$, also ein Faktor ϱ verbunden vorkommt, also mit k^n nothwendig der Faktor ϱ^n, statt dessen, wenn $n > \lambda - 1$ ist, auch $\lambda\varrho^{n-\lambda+1}$ genommen werden kann. Jedes Glied, welches k^n enthält, ist also, wenn $n > \lambda - 1$ ist, durch $\lambda\varrho$ theilbar, und weil das entwickelte Produkt die Wurzel α nicht enthält, so kann das mit k^n behaftete Glied derselben nicht durch $\lambda\varrho$ theilbar sein, ohne durch λ^2 theilbar zu sein. Bei der Untersuchung des Ausdrucks $\Phi(x, k)$ in Beziehung auf den Modul λ^2 kann man also alle Glieder, welche k^λ und höhere Potenzen des k enthalten, als durch λ^2 theilbar vernachlässigen. Ich entwickele nun den Logarithmus

$$l\phi(x + k(\alpha^r - 1)) = l\phi(x) + \frac{(\alpha^r - 1)k}{1}\,\frac{dl\phi(x)}{dx} + \frac{(\alpha^r - 1)^2 k^2}{1.\,2.}\,\frac{d^2 l\phi(x)}{dx^2} + \\ + \dots + k^\lambda A,$$

wo $k^\lambda A$ den Rest der Reihe vorstellt, vom λten Gliede an. Giebt man dem r die Werthe 0, 1, 2 ... $\lambda - 1$ und summirt, indem man bemerkt, dafs

$$(\alpha - 1)^n + (\alpha^2 - 1)^n + (\alpha^3 - 1)^n + \dots + (\alpha^{\lambda-1} - 1)^n = (-1)^n \lambda$$

ist, für alle Werthe des n, welche kleiner als λ sind, so erhält man:

$$(2.) \qquad l\Phi(x,k) = \lambda\Big\{l\Phi(x) - \frac{k}{1}\,\frac{dl\phi(x)}{dx} + \frac{k^2}{1.\,2.}\,\frac{d^2 l\phi(x)}{dx^2} - \dots + \\ + \frac{k^{\lambda-1}}{1.\,2.\,\dots(\lambda-1)}\,\frac{d^{\lambda-1} l\phi(x)}{dx^{\lambda-1}}\Big\} + k^\lambda B$$

Entwickelt man nun den Logarithmus von $\phi(x + k(e^v - 1))$ in eine nach Potenzen von k geordnete Reihe, und nimmt von dieser den $\lambda - 1$ten Differenzialquotienten nach v, für den besonderen Werth $v = 1$, so erhält man:

$$\frac{d_0^{\lambda-1} l\phi(x + k(e^v - 1))}{dv^{\lambda-1}} = \frac{k}{1}\,\frac{dl\phi(x)}{dx} + \frac{(2^{\lambda-1} - 2.\,1^{\lambda-1})k^2}{1.\,2.}\,\frac{d^2 l\phi(x)}{dx^2} + \\ \frac{(3^{\lambda-1} - 3.\,2^{\lambda-1} + 3.\,1^{\lambda-1})k^3}{1.\,2.\,3.}\,\frac{d^3 l\phi(x)}{dx^3} + \dots$$

welche Reihe eine endliche ist, und nur $\lambda - 1$ Glieder hat. Die Zahlencoefficienten, welche die $\lambda - 1$ten Differenzialquotienten von $(e^v - 1)^n$ sind, für $v = 0$, sind abwechselnd congruent $+1$ und -1, nach dem Modul λ, man hat daher:

$$(3.) \qquad \frac{d_0^{\lambda-1} l\phi(x + k(e^v - 1))}{dv^{\lambda-1}} = \frac{k}{1}\,\frac{dl\phi(x)}{dx} - \frac{k^2}{1.\,2.}\,\frac{d^2 l\phi(x)}{dx^2} + \\ + \dots - \frac{k^{\lambda-1}}{1.\,2.\,\dots(\lambda-1)}\,\frac{d^{\lambda-1} l\phi(x)}{dx^{\lambda-1}} + \lambda P,$$

wo P eine ganze rationale Funktion von k, des $\lambda - 1$ten Grades ist, deren Zahlencoefficienten, insofern sie Brüche sind, in den Nennern kein λ enthalten. Die Vergleichung der beiden Ausdrücke (2.) und (3.) giebt:

$$l\Phi(x,k) = \lambda l\phi(x) - \lambda\,\frac{d_0^{\lambda-1} l\phi(x + k(e^v - 1))}{dv^{\lambda-1}} + \lambda^2 P + k^\lambda B.$$

Nimmt man nun die Exponentialgröfsen und entwickelt, indem man die Glieder wegläfst, welche λ^2 und die welche k^λ oder höhere Potenzen von k enthalten, so hat man

$$(4.)\qquad \Phi(x,k) \equiv \phi(x)^\lambda \left(1 - \lambda \frac{d_0^{\lambda-1} l\phi\left(x+k(e^v-1)\right)}{dv^{\lambda-1}}\right), \text{ mod. } \lambda^2,$$

und demnach für $k = x$:

$$(5.)\qquad \phi(x)\,\phi(x\alpha)\,\ldots\,\phi(x\alpha^{\lambda-1}) \equiv \phi(x)^\lambda\left(1 - \frac{d_0^{\lambda-1} l\phi(xe^v)}{dv^{\lambda-1}}\right), \text{ mod. } \lambda^2.$$

Wenn die Coefficienten von $\phi(x)$ ganze Zahlen sind, deren Summe nicht durch λ theilbar ist, so hat man hieraus, wenn man $x = 1$ setzt und durch $\phi(1)$ dividirt:

$$(6.)\qquad N\phi(\alpha) \equiv \phi(1)^{\lambda-1}\left(1 - \lambda \frac{d_0^{\lambda-1} l\phi(e^v)}{dv^{\lambda-1}}\right), \text{ mod. } \lambda^2.$$

für jede complexe Zahl in α, welche den Faktor ϱ nicht enthält. Hieraus folgt weiter, weil $\phi(1)^{\lambda-1} \equiv 1$, mod. λ, ist:

$$(7.)\qquad \frac{1-N\phi(\alpha)}{\lambda} \equiv \frac{d_0^{\lambda-1} l\phi(e^v)}{dv^{\lambda-1}} - \frac{\phi(1)^{\lambda-1}-1}{\lambda}, \text{ mod. } \lambda,$$

welches den gesuchten Ausdruck des oben mit $C_{\lambda-1}$ bezeichneten Charakters durch den Differenzialquotienten des Logarithmus giebt.

Es sei nun $F(w)$ eine wirkliche complexe Zahl in w, und $F(\alpha)$ die Norm derselben, welche nicht durch ϱ theilbar sein soll, also wenn

$$F(w) = A + A_1 w + A_2 w^2 + \ldots + A_{\lambda-1} w^{\lambda-1}$$

gesetzt wird,

$$A + A_1 + A_2 + \ldots + A_{\lambda-1} \text{ nicht} \equiv 0, \text{ mod. } \varrho.$$

Es seien ferner $a, a_1, a_2 \,..\, a_{\lambda-1}$ die nichtcomplexen ganzen Zahlen, welchen die complexen Coefficienten $A, A_1, A_2, \ldots A_{\lambda-1}$ congruent sind, nach dem Modul ϱ, und

$$\phi(w) = a + a_1 w + a_2 w^2 + \ldots a_{\lambda-1} w^{\lambda-1},$$

so hat man:

$$F(w) = \phi(w) + \varrho\psi(w),$$

wo $\psi(w)$ irgend eine complexe Zahl in w ist, aus welcher Gleichung ohne Schwierigkeit die Congruenz

$$(8.)\qquad NF(w) \equiv N\phi(w), \text{ mod. } \lambda\varrho,$$

gefolgert wird. Entwickelt man nun die Norm von $\phi(w)$, und zwar so, daſs in dieser Entwickelung vorläufig w als eine beliebige unbestimmte Gröſse

betrachtet wird, so erhält man, von dem Fermatschen Satze $a^\lambda \equiv a$, mod. λ, Gebrauch machend, folgende Form:

$$(9.) \qquad N\phi(w) = a + a_1 w^\lambda + a^2 w^{2\lambda} + \dots a_{\lambda-1} w^{(\lambda-1)\lambda} + \lambda R(w^\lambda),$$

wo alle durch λ theilbaren Glieder als $\lambda R(w^\lambda)$ zusammengefaſst sind. Bezeichnet man nun mit $g(\alpha)$ die ganze complexe Zahl:

$$g(\alpha) = a + a_1 \alpha + a_2 \alpha^2 + \dots + a^{\lambda-1} \alpha^{\lambda-1},$$

und nimmt $w = 1$, so giebt diese Gleichung:

$$(10.) \qquad g(1)\, Ng(\alpha) = g(1) + \lambda R(1).$$

Giebt man aber dem w in der Gleichung (9.) seinen Werth als Wurzel der Gleichung $w^\lambda = D(\alpha)$, und macht aus derselben eine Congruenz nach dem Modul $\lambda\varrho$, so erhält man, weil $w^\lambda \equiv 1$, mod. ϱ ist, indem man für $N\phi(w)$ den nach dem Modul $\lambda\varrho$ congruenten Werth $NF(w) = F(\alpha)$ setzt:

$$(11.) \qquad \begin{aligned} F(\alpha) \equiv a + a_1 D(\alpha) + a_2 D(\alpha)^2 + \dots + a_{\lambda-1} D(\alpha)^{\lambda-1} + \\ + \lambda R(1), \text{ mod. } \lambda\varrho. \end{aligned}$$

Die Determinante hat nach der Voraussetzung die Eigenschaft, $D(\alpha) \equiv 1$, mod. ϱ, also für $\alpha = 1$, $D(1) \equiv 1$, mod. λ, man kann daher $D(1) = 1$ nehmen. Hierdurch wird vermöge der Congruenz (11.)

$$F(1) \equiv g(1) + \lambda R(1), \text{ mod. } \lambda^2,$$

und wenn zur $\lambda - 1$ten Potenz erhoben wird:

$$F(1)^{\lambda-1} \equiv g(1)^{\lambda-1} - \lambda g(1)^{\lambda-2} R(1), \text{ mod. } \lambda^2,$$

also

$$\frac{F(1)^{\lambda-1} - 1}{\lambda} \equiv \frac{g(1)^{\lambda-1} - 1}{\lambda} - g(1)^{\lambda-2} R(1), \text{ mod. } \lambda,$$

oder wenn für $R(1)$ sein Werth aus der Gleichung (10.) gesetzt wird; weil $g(1)^{\lambda-1} \equiv 1$, mod. λ ist:

$$\frac{F(1)^{\lambda-1} - 1}{\lambda} \equiv \frac{g(1)^{\lambda-1} - 1}{\lambda} + \frac{1 - Ng(\alpha)}{\lambda}, \text{ mod. } \lambda.$$

Vermöge der Congruenz (7.) erhält man hieraus

$$\frac{F(1)^{\lambda-1} - 1}{\lambda} \equiv \frac{d_0^{\lambda-1} lg(e^v)}{dv^{\lambda-1}}, \text{ mod. } \lambda,$$

und weil nach derselben Congruenz (7.)

$$C_{\lambda-1} \equiv \frac{1-NF(\alpha)}{\lambda} \equiv \frac{d_0^{\lambda-1} lF(e^v)}{dv^{\lambda-1}} - \frac{F(1)^{\lambda-1}-1}{\lambda}, \text{ mod. } \lambda,$$

so hat man endlich

$$(12.) \qquad C^1_{\lambda-1} \equiv \frac{d_0^{\lambda-1} lF(e^v)}{dv^{\lambda-1}} - \frac{d_0^{\lambda-1} lg(e^v)}{dv^{\lambda-1}}.$$

Ich bezeichne nun auch diejenigen Differenzialquotienten des Logarithmus von $F(e^v)$, welche nicht als Charaktere auftreten, ebenfalls mit C und dem entsprechenden Index, so dafs

$$C_n \equiv \frac{d_0^n lF(e^v)}{dv^n}, \text{ mod. } \lambda,$$

ist, für alle Werthe des $n = 1, 2, 3, \ldots \lambda - 2$. Ferner bezeichne ich die Differenzialquotienten des Logarithmus der Determinante $D(\alpha)$ mit dem Buchstaben D und dem zugehörigen Index, so dafs

$$D_n \equiv \frac{d_0^n lD(e^v)}{dv^n}, \text{ mod. } \lambda,$$

ist, für alle Werthe des $n = 1, 2, 3, \ldots \lambda - 2$ und

$$D_{\lambda-1} \equiv \frac{1-ND(\alpha)}{\lambda}, \text{ mod. } \lambda,$$

welcher Ausdruck vermöge der Congruenz (7.), da $D(1) = 1$ ist,

$$D_{\lambda-1} \equiv \frac{d_0^{\lambda-1} lD(e^v)}{dv^{\lambda-1}}, \text{ mod. } \lambda,$$

giebt.

Ich mache jetzt von den bekannten Formeln der Differenzialrechnung Gebrauch, welche zeigen, wie die Differenzialquotienten der Funktion einer Funktion gefunden werden. Sei y eine Funktion von x, und x eine Funktion von v, so hat man:

$$\frac{dy}{dv} = \frac{dx}{dv}\frac{dy}{dx}$$

$$(13.) \qquad \frac{d^2y}{dv^2} = \frac{d^2x}{dv^2}\frac{dy}{dx} + \left(\frac{dx}{dv}\right)^2 \frac{d^2y}{dx^2}$$

$$\frac{d^3y}{dx^3} = \frac{d^3x}{dv^3}\frac{dy}{dx} + 3\frac{dx}{dv}\frac{d^2x}{dv^2}\frac{d^2y}{dx^2} + \left(\frac{dx}{dv}\right)^3 \frac{d^3y}{dx^3}$$

und allgemein

$$\frac{d^ny}{dx^n} = V_1 \frac{dy}{dx} + V_2 \frac{d^2y}{dx^2} + V_3 \frac{d^3y}{dx^3} + \ldots + V_n \frac{d^ny}{dx^n}.$$

Die Gröfsen $V_1, V_2, \ldots V_n$ können nach bekannten Regeln auf combinatorischem Wege für jeden Werth des n gefunden werden. Aus diesen Regeln ergiebt sich auch, was hier von Wichtigkeit ist, dafs wenn $n = \lambda$ eine Primzahl ist, die Ausdrücke $V_2, V_3, \ldots V_{\lambda-1}$ in allen ihren Gliedern den numerischen Faktor λ haben. Aufserdem ist zu bemerken, dafs für $n = \lambda$, $V_1 = \frac{d^\lambda x}{dv^\lambda}$ und $V_\lambda = \left(\frac{dx}{dv}\right)^\lambda$ ist.

Ich setze nun $y = lF(e^v)$ und $x = lD(e^v)$. Es ist so y in der That eine Funktion von x, wenn man den Ausdruck aus Congruenz (11.):

$$F(\alpha) \equiv a + a_1 D(\alpha) + a_2 D(\alpha)^2 + \ldots + a_{\lambda-1} D(\alpha)^{\lambda-1}, \text{ mod. } \lambda,$$

anwendet. Für diese Werthe des y und x geben die Gleichungen (13.), wenn nach geschehener Differenziation $v = 0$ gesetzt wird, und wenn der Kürze wegen noch

$$\frac{d_0^n \, lg(e^v)}{dv^n} = g_n,$$

für $n = 1, 2, 3, \ldots \lambda - 1$, gesetzt wird:

$$\begin{aligned}
C_1 &\equiv D_1 g_1 \\
C_2 &\equiv D_2 g_1 + D_1^2 g_2 \\
C_3 &\equiv D_3 g_1 + 3D_1 D_2 g_2 + D_1^3 g_3 \\
&\vdots \\
C_{\lambda-1} + g_{\lambda-1} &\equiv D_{\lambda-1} g_1 + V_2 g_2 + V_3 g_3 + \ldots + D_1^{\lambda-1} g_{\lambda-1}.
\end{aligned}$$

Aus der schon oben festgesetzten Bedingung, dafs $D(\alpha) - 1$ den Faktor ϱ einmal, aber nicht öfter enthalten soll, folgt, dafs $D(e^v) = 1 + (1 - e^v)\psi(e^v)$ ist, wo $\psi(e^v)$, für $v = 0$, nicht congruent Null ist, man hat daher $D_1 = \frac{d_0 lD(e^v)}{dv}$ offenbar nicht congruent Null, nach dem Modul λ, und folglich $D_1^{\lambda-1} \equiv 1$, mod. λ. Wegen dieser Congruenz fällt die Gröfse $g_{\lambda-1}$ aus der letzten Congruenz von selbst weg und man hat $\lambda - 1$ Congruenzen, aus welchen die $\lambda - 2$ Gröfsen $g_1, g_2, g_3 \ldots g_{\lambda-2}$ zu eliminiren sind, um die gesuchte Congruenz unter den Gröfsen $C_1, C_2, C_3 \ldots C_{\lambda-1}$ zu erhalten.

Diese Elimination wird am leichtesten auf folgende Weise ausgeführt. In der allgemeinen Formel (13.) setze man:

$$y = \int lF(e^v) \frac{dx}{dv} \cdot dv, \quad x = lD(e^v),$$

so hat man für $n = \lambda$ und $v = 0$:

$$(15.)\quad \frac{d_0^{\lambda-1}\left(lF(e^v)\frac{dlD(e^v)}{dv}\right)}{dv^{\lambda-1}} = V_1 lF(1) + V_2 g_2 + V_3 g_3 + \dots + \\ + V_\lambda g_{\lambda-1},$$

entwickelt man nun denselben Differenzialquotienten nach der bekannten Formel für die Differenziation eines Produkts von zwei Faktoren, so erhält man für $v = 0$, indem man von den oben festgesetzten Bezeichnungen der Differenzialquotienten von $lF(e^v)$ und $lD(e^v)$ Gebrauch macht:

$$(16.)\quad \frac{d_0^{\lambda-1}\left(lF(e^v)\frac{dlD(e^v)}{dv}\right)}{dv^{\lambda-1}} = \frac{d_0^\lambda lD(e^v)}{dv^\lambda}\, lF(1) + \frac{\lambda-1}{1} D_{\lambda-1} C_1 + \\ + \frac{(\lambda-1)(\lambda-1)}{1.\,2} D_{\lambda-2} C_2 + \dots + D_1 (C_{\lambda-1} + g_{\lambda-1}).$$

Vergleicht man nun diese beiden Ausdrücke mit einander, indem man beachtet, dafs

$$V_1 = \frac{d_0^\lambda\, lD(e^v)}{dv^\lambda},\quad V_\lambda = D_1^\lambda,$$

und dafs $V_2, V_3, \dots V_{\lambda-1}$ alle den Faktor λ enthalten, so erhält man, wenn man die Vielfachen von λ wegläfst, folgende Congruenz:

$$(17.)\quad D_{\lambda-1} C_1 - D_{\lambda-2} C_2 + D_{\lambda-3} C_3 - \dots - D_1 C_{\lambda-1} \equiv 0, \text{ mod. } \lambda,$$

welches die gesuchte Congruenz ist.

Es soll nun gezeigt werden, dafs diese Congruenz auch die einzige Bedingung enthält, welche diese Gröfsen $C_1, C_2, \dots C_{\lambda-1}$ erfüllen müssen, damit eine wirkliche Zahl $F(w)$ existire, deren Norm $F(\alpha)$ irgend welche gegebene Werthe der Gröfsen $C_1, C_2, \dots C_{\lambda-1}$ habe.

Wenn in den ersten $\lambda - 2$ Congruenzen bei (14.) die $\lambda - 2$ Gröfsen $C_1, C_2, \dots C_{\lambda-2}$ als gegebene betrachtet werden, so lassen sich durch dieselben die $\lambda - 2$ Gröfsen $g_1, g_2, \dots g_{\lambda-2}$ vollständig bestimmen, weil D_1 nicht congruent Null ist, durch diese Gröfsen $g_1, g_2, \dots g_{\lambda-2}$ werden nun weiter die Zahlen $a, a_1, a_2, \dots a_{\lambda-1}$ in folgender Weise bestimmt: Man hat, wenn u irgend eine Funktion von v ist, unter den Differenzialquotienten von u und denen des Logarithmus von u folgende Gleichungen:

$$(18.)\quad \begin{aligned} \frac{du}{dv} &= u\frac{dlu}{dv} \\ \frac{d^2u}{dv^2} &= \frac{du}{dv}\,\frac{dlu}{dv} + u\,\frac{d^2lu}{dv^2} \\ \frac{d^3u}{dv^3} &= \frac{d^2u}{dv^2}\,\frac{dlu}{dv} + 2\,\frac{du}{dv}\,\frac{d^2lu}{dv^2} + u\,\frac{d^3lu}{dv^3} \end{aligned}$$

u. s. w.

Nimmt man nun $u = g(e^v)$ und setzt nach geschehener Differenziation $v = 0$, so hat man, indem man von der Bezeichnung der Differenzialquotienten des Logarithmus von $g(e^v)$ durch $g_1, g_2, \dots g_{\lambda-1}$ Gebrauch macht, und aufserdem der Kürze wegen

$$\frac{d^n_0 g(e^v)}{dv^n} = b_n$$

nimmt, folgende Gleichungen:

$$(19.)\quad \begin{aligned} b_1 &= b_0 g_1 \\ b_2 &= b_1 g_1 + b_0 g_2 \\ b_3 &= b_2 g_1 + 2 b_1 g_2 + b_0 g_3 \\ &\vdots \\ b_{\lambda-2} &= b_{\lambda-3} g_1 + \frac{\lambda-3}{1}\, b_{\lambda-4} g_2 + \frac{(\lambda-3)(\lambda-4)}{1.2}\, b_{\lambda-5} g_3 + \dots \\ &\quad + b_0 g_{\lambda-2}. \end{aligned}$$

Vermittelst dieser Gleichungen, welche man auch blofs als Congruenzen nach dem Modul λ aufzufassen braucht, kann man nun, wenn $g_1, g_2, \dots g_{\lambda-2}$ gegeben sind, die Gröfsen $b_1, b_2, \dots b_{\lambda-2}$ vollständig bestimmen, wobei der Werth des b_0 unbestimmt bleibt. Endlich hat man aus dem Ausdrucke des $g(\alpha)$:

$$g(e^v) = a + a_1 e^v + a_2 e^{2v} + \dots + a_{\lambda-1} e^{(\lambda-1)v}$$

die Congruenzen:

$$(20.)\quad \begin{aligned} b_0 - a &\equiv a_1 + a_2 + a_3 + \dots + a_{\lambda-1} \\ b_1 &\equiv 1 a_1 + 2 a_2 + 3 a_3 + \dots + (\lambda-1) a_{\lambda-1} \\ b_2 &\equiv 1^2 a_1 + 2^2 a_2 + 3^2 a_3 + \dots + (\lambda-1)^2 a_{\lambda-1} \\ &\vdots \\ b_{\lambda-2} &\equiv 1^{\lambda-2} a_1 + 2^{\lambda-2} a_2 + 3^{\lambda-2} a_3 + \dots + (\lambda-1)^{\lambda-2} a_{\lambda-1}, \end{aligned}$$

aus denen, weil die Determinante dieses Systems nicht durch λ theilbar ist, die Zahlen $a_1, a_2, \dots a_{\lambda-1}$ vermittelst der gegebenen $b_1, b_2, \dots b_{\lambda-2}$ be-

stimmt werden, wobei a zugleich mit b_0 unbestimmt bleibt. Für alle gegebenen Werthe von C_1, C_2, C_3 ... $C_{\lambda-2}$ giebt es darum stets zugehörige Werthe der Zahlen a, a_1, a_2 ... $a_{\lambda-1}$, und demnach auch zugehörige Werthe der A, A_1, A_2 ... $A_{\lambda-1}$, welche nur dadurch bestimmt sind, dafs sie den Zahlen a, a_1, a_2 ... $a_{\lambda-1}$ nach dem Modul ϱ congruent sein müssen. Es giebt also auch wirkliche complexe Zahlen

$$F(w) = A + A_1 w + A_2 w^2 + \ldots + A_{\lambda-1} w^{\lambda-1},$$

welchen die Gröfsen C_1, C_2, ... $C_{\lambda-2}$ angehören, für alle Werthe, die man denselben beilegen mag, und wenn die letzte dieser Gröfsen $C_{\lambda-1}$ aus den übrigen durch die Congruenz (17.) bestimmt ist, so gehört auch diese der complexen Zahl $F(w)$ an. Das Resultat dieser ganzen Untersuchung ist in dem folgenden Satze enthalten:

(I.) Wenn eine complexe Zahl $F(\alpha)$ die Norm einer wirklichen complexen Zahl in w, der Determinante $D(\alpha)$ ist, so mufs sie der Congruenz

$$D_{\lambda-1} C_1 - D_{\lambda-2} C_2 + D_{\lambda-3} C_3 - \ldots - D_1 C_{\lambda-1} \equiv 0, \quad \text{mod. } \lambda,$$

genügen, in welcher

$$C_n = \frac{d^n_0 \, l\, F(e^v)}{dv^n}, \quad D_n = \frac{d^n_0 \, l\, D(e^v)}{dv^n},$$

für $n = 1, 2, 3, \lambda - 2$ und

$$C_{\lambda-1} = \frac{1 - NF(\alpha)}{\lambda}, \quad D_{\lambda-1} = \frac{1 - ND(\alpha)}{\lambda},$$

und wenn die Zahlenwerthe der Gröfsen C_1, C_2, C_3, ... $C_{\lambda-1}$ irgend wie gegeben sind, mit der alleinigen Bedingung, dafs sie dieser Congruenz genügen, so kann man stets eine wirkliche complexe Zahl $F(w)$ der Determinante $D(\alpha)$ angeben, deren Norm $F(\alpha)$ diese gegebenen Zahlenwerthe der Gröfsen C_1, C_2, C_3, ... $C_{\lambda-1}$ hat.

Die Congruenz (17.), welche für die Theorie der complexen Zahlen in w von grofser Bedeutung ist, und namentlich dadurch sich auszeichnet, dafs die Norm $F(\alpha)$ und die Determinante $D(\alpha)$ in denselben vollkommen symmetrisch vorkommen, kann auch in eine andere höchst einfache Form gebracht werden, welche ich mit Hülfe eines in meiner Abhandlung über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen,

Crelle's Journal, Bd. 44. bewiesenen Satzes hier entwickeln will. Ich habe daselbst, pag. 144, folgende Formel bewiesen:

$$\text{Ind. } \phi(\alpha) \equiv \text{Ind. } \phi_1(\alpha) + \sum_0^{\mu-1} \frac{d_0^{2n}\, l\phi(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n}\, lf(e^v)}{dv^{\lambda-2n}}, \text{ mod. } \lambda,$$

in welcher $\phi(\alpha)$ eine beliebige complexe Zahl ist, die nur der einen Bedingung unterworfen ist, dafs sie einer nichtcomplexen, von Null verschiededenen Zahl congruent ist, nach dem Modul ϱ^2, und $\phi_1(\alpha)$ dieselbe Zahl darstellt als $\phi(\alpha)$, aber primär genommen, wo ferner das Zeichen des Index: Ind. auf die Primzahl $f(\alpha)$ sich beziehend, durch die Gleichung

$$\left(\frac{\phi(\alpha)}{f(\alpha)}\right) = \alpha^{\text{ Ind. } \phi(\alpha)}$$

definirt ist. Es ist nun für den gegenwärtigen Zweck nöthig, die complexe Zahl $\phi(\alpha)$ auch noch von der einen ihr auferlegten Beschränkung zu befreien, dafs sie nach dem Modul ϱ^2 einer nichtcomplexen Zahl congruent sein soll, welches geschieht, indem sie mit einer beliebigen Potenz von α multiplicirt wird. Man hat

$$\text{Ind. } (\alpha^k\, \phi(\alpha)) \equiv \text{Ind. } \phi(\alpha) + k \text{ Ind. } (\alpha),$$

ferner ist

$$\frac{d_0\, l(e^{vk}\, \phi(e^v))}{dv} \equiv k, \quad \frac{d_0^{2n}\, l(e^{vk}\, \phi(e^v))}{dv^{2n}} \equiv \frac{d_0^{2n}\, l\phi(e^v)}{dv^{2n}},$$

und weil nach der Definition des Legendreschen Zeichens oder des Index

$$\text{Ind. } (\alpha) \equiv \frac{Nf(\alpha)-1}{\lambda}$$

ist, so hat man, wenn anstatt $\alpha^k\, \phi(\alpha)$ einfach $\phi(\alpha)$ geschrieben wird:

$$(21.) \qquad \text{Ind. } \phi(\alpha) \equiv \text{Ind. } \phi_1(\alpha) - \frac{d_0\, l\phi(e^v)}{dv}\left(\frac{1-Nf(\alpha)}{\lambda}\right) + \\ + \sum_0^{\mu-1} \frac{d_0^{2n}\, l\phi(e^v)}{dv^{2n}} \frac{d_0^{\lambda-2n}\, lf(e^v)}{dv^{\lambda-2n}},$$

in welcher Formel $\phi(\alpha)$ eine jede beliebige (nicht durch ϱ theilbare) complexe Zahl ist, und $\phi_1(\alpha)$ dieselbe in der primären Form.

Verallgemeinert man nun das Legendresche Zeichen in der Art, dafs es auch auf zusammengesetzte Moduln anwendbar ist, indem man definirt, dafs wenn $\psi(\alpha) = E(\alpha)\, f(\alpha)^m\, f_1(\alpha)^{m_1}\, f_2(\alpha)^{m_2} \ldots$ ist, wo $E(\alpha)$ eine Einheit bezeichnet,

$$\left(\frac{\phi(\alpha)}{\psi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right)^{m} \left(\frac{\phi(\alpha)}{f_1(\alpha)}\right)^{m_1} \left(\frac{\phi(\alpha)}{f_2(\alpha)}\right)^{m_2} \cdots$$

sein soll, und verallgemeinert man demgemäfs auch das Zeichen des Index Ind., so dafs es auch für die zusammengesetzte Zahl $\psi(\alpha)$ durch die Gleichung

$$\left(\frac{\phi(\alpha)}{\psi(\alpha)}\right) = \alpha^{\text{Ind. } \phi(\alpha)}$$

definirt ist, und bemerkt, dafs für den angegebenen Werth des $\psi(\alpha)$

$$\frac{d_0^n l\psi(e^v)}{dv^n} \equiv m \frac{d_0^n lf(e^v)}{dv^n} + m_1 \frac{d_0^n lf_1(e^v)}{dv^n} + \cdots\cdots$$

$$\frac{1-N\psi(\alpha)}{\lambda} \equiv m \frac{1-Nf(\alpha)}{\lambda} + m_1 \frac{1-Nf_1(\alpha)}{\lambda} + \cdots\cdots$$

so erhält man die allgemeinere, für alle beliebigen, nicht durch ϱ theilbaren Zahlen $\phi(\alpha)$ und $\psi(\alpha)$ geltende Congruenz:

$$\text{(22.)} \qquad \text{Ind. } \phi(\alpha) \equiv \text{Ind. } \phi_1(\alpha) - \frac{d_0 l\phi(e^v)}{dv} \cdot \frac{1-N\psi(\alpha)}{\lambda} + \\ + \sum_{1}^{\mu-1}{}_n \frac{d_0^{2n} l\phi(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n} l\psi(e^v)}{dv^{\lambda-2n}},$$

welche auch so dargestellt werden kann:

$$\text{(23.)} \qquad \left(\frac{\phi(\alpha)}{\psi(\alpha)}\right) = \left(\frac{\phi_1(\alpha)}{\psi(\alpha)}\right) \alpha^{\Sigma},$$

wo

$$\Sigma \equiv -\frac{d_0 l\phi(e^v)}{dv} \cdot \frac{1-N\psi(\alpha)}{\lambda} + \\ + \sum_{1}^{\mu-1}{}_n \frac{d_0^{2n} l\phi(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n} l\psi(e^v)}{dv^{\lambda-2n}}, \quad \text{mod. } \lambda.$$

Diese Formel giebt auch einen neuen Ausdruck für den Index einer beliebigen Einheit $E(\alpha)$. Nimmt man nämlich in derselben $\phi_1(\alpha) = 1$, so ist $\phi(\alpha)$ eine ganz beliebige Einheit $E(\alpha)$, und man hat:

$$\text{(24.)} \qquad \text{Ind. } E(\alpha) \equiv -\frac{d_0 l E(e^v)}{dv} \cdot \frac{1-N\psi(\alpha)}{\lambda} + \\ + \sum_{1}^{\mu-1}{}_n \frac{d_0^{2n} l E(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n} l\psi(e^v)}{dv^{\lambda-2n}},$$

oder was dasselbe ist:

(25.) $$\left(\frac{E(\alpha)}{\psi(\alpha)}\right) = \alpha^{\frac{-d_0 lE(e^v)}{dv} \cdot \frac{1-N\psi(\alpha)}{\lambda} + \sum_1^{\mu-1}{}_n \frac{d_0^{2n} lE(e^v)}{dv^{2n}} \cdot \frac{d_0^{\lambda-2n} l\psi(e^v)}{dv^{\lambda-2n}}}$$

Um nun die gefundene Formel (22.) auf die Umformung der Congruenz (17.) anzuwenden, nehme ich zunächst $\phi(\alpha) = F(\alpha)$, $\psi(\alpha) = D(\alpha)$, und setze $F(\alpha) = E(\alpha) F_1(\alpha)$, wo $F_1(\alpha)$ primär sein soll, und $E(\alpha)$ eine Einheit ist. Für diese Zahlen $F(\alpha)$ und $D(\alpha)$ giebt die Congruenz (22.) unter Anwendung der eingeführten Zeichen für die Differenzialquotienten der Logarithmen der betreffenden complexen Zahlen:

(26.) $$\text{ind. } E(\alpha) \equiv -C_1 D_{\lambda-1} + C_2 D_{\lambda-2} + C_4 D_{\lambda-4} + \dots + C_{\lambda-3} D_3,$$

wo das Zeichen des Index: ind. auf den Modul $D(\alpha)$ sich bezieht. Setzt man zweitens in der Formel (22.) $\phi(\alpha) = D(\alpha)$, $\psi(\alpha) = F(\alpha)$ und $D(\alpha) = \varepsilon(\alpha) D_1(\alpha)$, wo $D_1(\alpha)$ primär sein soll, und $\varepsilon(\alpha)$ diejenige Einheit, welche aus $D(\alpha)$ herausgehoben werden mufs, damit es primär werde, so hat man:

(27.) $$\text{Ind. } \varepsilon(\alpha) \equiv -D_1 C_{\lambda-1} + D_2 C_{\lambda-2} + D_4 C_{\lambda-4} + \dots + D_{\lambda-3} C_3,$$

wo der Index: Ind. auf den Modul $F(\alpha)$ sich bezieht. Vergleicht man endlich die beiden Ausdrücke des ind. $E(\alpha)$ und des Ind. $\varepsilon(\alpha)$ mit der Congruenz (17.), so hat man die gesuchte Umformung derselben, nämlich:

(28.) $$\text{ind. } E(\alpha) \equiv \text{Ind. } \varepsilon(\alpha), \quad \text{mod. } \lambda,$$

welche in den Legendreschen Zeichen so ausgedrückt wird:

(29.) $$\left(\frac{E(\alpha)}{D(\alpha)}\right) = \left(\frac{\varepsilon(\alpha)}{F(\alpha)}\right).$$

Dieses Resultat kann nun vollständig so ausgesprochen werden:

(II.) Die Congruenz, welcher eine jede complexe Zahl $F(\alpha)$ genügen mufs, wenn sie als Norm einer wirklichen complexen Zahl in w der Determinante $D(\alpha)$ darstellbar ist, nämlich:

$$D_{\lambda-1} C_1 - D_{\lambda-2} C_2 + D_{\lambda-3} C_3 - \dots - D_1 C_{\lambda-1} \equiv 0, \quad \text{mod. } \lambda,$$

ist gleichbedeutend mit der Gleichung:

$$\left(\frac{E(\alpha)}{D(\alpha)}\right) = \left(\frac{\varepsilon(\alpha)}{F(\alpha)}\right),$$

in welcher $E(\alpha)$ und $\varepsilon(\alpha)$ diejenigen Einheiten bezeichnen, welche durch die Gleichungen

$$F(\alpha) = E(\alpha) F_1(\alpha), \quad D(\alpha) = \varepsilon(\alpha) D_1(\alpha)$$

bestimmt werden, in denen $F_1(\alpha)$ und $D_1(\alpha)$ primär sind.

§. 15.

Sätze über die genaue Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in z.

In den jetzt folgenden Untersuchungen wird eine besondere Art von complexen Primzahlen in α auftreten, welche in einigen allgemeinen Sätzen Ausnahmen begründen, oder doch eine besondere Behandlung erfordern, nämlich die complexen Primzahlen, welche die besondere Eigenschaft haben, dafs alle Einheiten für sie λte Potenzreste sind. Wenn $\psi(\alpha)$ eine complexe Primzahl dieser besonderen Art ist, so zeigt der bei (24.) §. 14. gegebene Ausdruck des Index einer beliebigen Einheit, dafs für dieselbe die Ausdrücke

$$\frac{d_0^3 l\psi(e^v)}{dv^3}, \quad \frac{d_0^5 l\psi(e^v)}{dv^5}, \quad \ldots \quad \frac{d_0^{\lambda-2} l\psi(e^v)}{dv^{\lambda-2}}, \quad \frac{1-N\psi(\alpha)}{\lambda},$$

alle einzeln congruent Null sein müssen, nach dem Modul λ, und umgekehrt, wenn diese Ausdrücke alle congruent Null sind, dafs jede beliebige Einheit $E(\alpha)$ ein λter Potenzrest von $\psi(\alpha)$ ist. In Rücksicht auf dieses Verhalten gegen die Einheiten unterscheide ich darum zwei verschiedene Arten von complexen Primzahlen, und nenne diejenigen complexen Primzahlen in α, welche die besondere Eigenschaft haben, dafs für sie alle Einheiten in α λte Potenzreste sind: complexe Primzahlen der zweiten Art, diejenigen aber, welche diese besondere Eigenschaft nicht haben, complexe Primzahlen der ersten Art.

Ich bemerke, dafs in der Theorie der quadratischen Reste, wo es sich nur um gewöhnliche ganze Zahlen handelt, den hier als Primzahlen der ersten Art bezeichneten die Primzahlen von der Form $4n+3$ entsprechen, dagegen den als Primzahlen der zweiten Art bezeichneten die Primzahlen von der Form $4n+1$. Es giebt nämlich hier nur die beiden Einheiten $+1$ und -1, und diese sind für die Primzahlen der Form $4n+1$ beide quadratische Reste, für die Primzahlen der Form $4n+3$ aber ist -1 ein Nichtrest.

Ich wende nun den im vorigen Paragraphen gefundenen Satz (I.) auf die Bestimmung der genauen Anzahl der Gattungen der idealen Zahlen in z

an, und zwar zunächst für den Fall, dafs die Determinante $D(\alpha)$ nur **einen** Primfaktor enthält. Wenn die als Charaktere bezeichneten Gröfsen

$$C_3,\ C_5,\ C_7,\ \ldots\ C_{\lambda-2},\ C_{\lambda-1},$$

deren jede in Beziehung auf den Modul λ die Werthe $0, 1, 2, \ldots \lambda-1$ haben kann, irgend wie gegeben sind, so kann man, da noch die Gröfsen $C_1, C_2, C_4, \ldots C_{\lambda-3}$ verfügbar bleiben, diese im allgemeinen so wählen, dafs der Congruenz

$$D_{\lambda-1}C_1 - D_{\lambda-2}C_2 + D_{\lambda-3}C_3 - \ldots - D_1C_{\lambda-1} \equiv 0, \text{ mod. } \lambda,$$

genügt wird. Nur in dem einen besonderen Falle wird diefs nicht möglich sein, wenn von den Gröfsen $C_1, C_2, C_4, \ldots C_{\lambda-3}$ keine in dieser Congruenz vorkommt, also nur dann, wenn die Determinante $D(\alpha)$ so beschaffen ist, dafs für dieselbe die Gröfsen

$$D_3,\ D_5,\ D_7,\ \ldots\ D_{\lambda-2},\ D_{\lambda-1}$$

alle einzeln congruent Null sind. In diesem Falle können die genannten Charaktere einer idealen Zahl in z, welche sich als wirkliche complexe Zahl in w darstellen läfst, nicht mehr alle beliebigen Werthe haben, sondern nur diejenigen Werthe, welche der Congruenz

$$(1.)\qquad D_{\lambda-3}C_3 + D_{\lambda-5}C_5 + \ldots + D_2C_{\lambda-2} - D_1C_{\lambda-1} \equiv 0, \text{ mod. } \lambda,$$

genügen. Für alle anderen Determinanten $D(\alpha)$ aber, welche nicht diese besondere Eigenschaft haben, kann man, wie auch die Charaktere $C_3, C_5, \ldots C_{\lambda-2}, C_{\lambda-1}$ gegeben sein mögen, stets wirkliche complexe Zahlen in w finden, welche, als ideale Zahlen in z betrachtet, diese gegebenen Charaktere haben. Da die Anzahl dieser Einzelcharaktere gleich $\mu = \frac{\lambda-1}{2}$ ist, und jeder die λ Werthe $0, 1, 2 \ldots \lambda-1$ haben kann, so folgt, dafs die Anzahl aller Werthverbindungen derselben gleich λ^μ ist, dafs also λ^μ Gattungen wirklich existiren, da man zu jeder derselben ideale Zahlen angeben kann, welche sie enthält. Da ferner nach dem Satze (IV.) §. 13, in dem vorliegenden Falle, wo die Determinante nicht mehr als **einen** Primfaktor enthält, nicht mehr als λ^μ Gattungen existiren, so folgt, dafs der mit K bezeichnete Charakter durch die Charaktere $C_3, C_5, \ldots C_{\lambda-1}$ vollständig bestimmt ist, so dafs alle idealen Zahlen in z, welche dieselben Werthe dieser Charaktere haben, auch denselben Werth des Charakters K haben müssen. Der Ausnahmefall, in welchem $D_3, D_5, \ldots D_{\lambda-1}$ alle congruent Null sind,

mod. λ, tritt nur dann, und immer dann ein, wenn die eine in der Determinante $D(\alpha)$ enthaltene Primzahl eine complexe Primzahl der zweiten Art ist, denn diese Bedingungen stimmen mit den oben für die Primzahlen der zweiten Art angegebenen vollständig überein. Man hat also folgende zwei Sätze:

(I.) Wenn die Determinante nur einen Primfaktor enthält, und zwar eine Primzahl der ersten Art, so ist die Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in z genau gleich λ^{μ}, also genau gleich dem λten Theile aller angebbaren Gesamtcharaktere, und der Charakter K ist durch die Charaktere C_3, C_5, ... $C_{\lambda-1}$ vollständig bestimmt.

(II.) Unter derselben Voraussetzung enthält jede wirklich vorhandene Gattung solche ideale Zahlen in z, welche sich als wirkliche complexe Zahlen in w darstellen lassen.

Es soll nun weiter auch in dem Falle, wo die Determinante zwei verschiedene Primfaktoren enthält, untersucht werden, in wie weit es gelingt, die $\lambda^{\mu+1}$ Gattungen, welche nach dem Satze (IV.), §. 13. noch Statt haben können, durch solche ideale Zahlen in z, welche sich als wirkliche complexe Zahlen in u, u_1 darstellen lassen, vollständig auszufüllen, und dadurch nachzuweisen, dafs die Anzahl der wirklich vorhandenen Gattungen in diesem Falle genau gleich $\lambda^{\mu+1}$ ist. Es sei nach der im §. 9. eingeführten Bezeichnung

$$(2.)\qquad \begin{gathered} u^{\lambda} = e(\alpha)f(\alpha)^{m}, \qquad u_1^{\lambda} = e_1(\alpha)f_1(\alpha)^{m_1} \\ D(\alpha) = u^{\lambda} u_1^{\lambda}, \qquad w = u u_1 \\ F(u, u_1) = \sum_0^{\lambda-1}{}_k\, A_k\, u^{|k-n|}\, u_1^{|k-n_1|} \end{gathered}$$

wo $|k-n|$ und $|k-n_1|$ die kleinsten nicht negativen Reste von $k-n$ und $k-n_1$, nach dem Modul λ, bezeichnen. Es sei ferner:

$$(3.)\qquad \begin{gathered} u^{n} u_1^{n_1} F(u, u_1) = F'(w) \\ NF'(w) = F'(\alpha), \qquad NF(u, u_1) = F(\alpha), \\ e(\alpha)f(\alpha)^{m} = d(\alpha), \qquad e_1(\alpha)f_1(\alpha)^{m_1} = \delta(\alpha), \end{gathered}$$

so ist

$$(4.)\qquad F'(\alpha) = d(\alpha)^{n}\,\delta(\alpha)^{n_1}\,F(\alpha).$$

Weil nun $F'(w)$ eine wirkliche complexe Zahl in w ist, deren Norm den Faktor ϱ nicht enthält, so findet für dieselbe die Congruenz des Satzes (I.) §. 14. Statt:

$$(5.)\quad D_{\lambda-1}C'_1 - D_{\lambda-2}C'_2 + D_{\lambda-3}C'_3 - \dots - D_1 C'_{\lambda-1} \equiv 0, \text{ mod. } \lambda,$$

in welcher

$$C'_k = \frac{d_0^k\, l F'(e^v)}{dv^k}, \quad C'_{\lambda-1} = \frac{1-NF'(\alpha)}{\lambda}$$

gesetzt ist. Bezeichnet man dem entsprechend die Differenzialquotienten der Logarithmen für die complexen Zahlen $d(\alpha)$ und $\delta(\alpha)$ durch

$$d_k = \frac{d_0^k\, l d(e^v)}{dv^k}, \quad d_{\lambda-1} = \frac{1-Nd(\alpha)}{\lambda},$$

$$\delta_k = \frac{d_0^k\, l \delta(e^v)}{dv^k}, \quad \delta_{\lambda-1} = \frac{1-N\delta(\alpha)}{\lambda},$$

so hat man vermöge der Gleichung (4.):

$$(6.)\qquad C'_k \equiv n d_k + n_1 \delta_k + C_k, \text{ mod. } \lambda,$$

und vermöge der Gleichung $D(\alpha) = d(\alpha)\,\delta(\alpha)$:

$$(7.)\qquad D_k \equiv d_k + \delta_k, \text{ mod. } \lambda,$$

für alle Werthe $k = 1, 2, 3, \dots \lambda - 1$. Setzt man diese Ausdrücke in die Congruenz (5.) ein, indem man der Einfachheit wegen die Summenzeichen gebraucht, so hat man

$$(8.)\qquad \sum_{1}^{\lambda-1}{}_k\, (-1)^k\, (d_{\lambda-k} + \delta_{\lambda-k})\,(C_k + n d_k + n_1 \delta_k) \equiv 0, \text{ mod. } \lambda,$$

und wenn die Multiplikation unter dem Summenzeichen ausgeführt wird:

$$\begin{aligned}\Sigma(-1)^k\,(d_{\lambda-k} + \delta_{\lambda-k})\,C_k + n\Sigma(-1)^k\, d_{\lambda-k}\, d_k + n\Sigma(-1)^k\, \delta_{\lambda-k}\, d_k \\ + n_1\Sigma(-1)^k\, d_{\lambda-k}\,\delta_k + n_1\Sigma(-1)^k\,\delta_{\lambda-k}\,\delta_k \equiv 0, \text{ mod. } \lambda.\end{aligned}$$

Die zweite und fünfte dieser Summen verschwinden von selbst, weil in ihnen die vom Anfange und vom Ende gleich weit entfernten Glieder gleich sind und entgegengesetzte Vorzeichen haben, die vierte Summe aber ist gleich der dritten mit entgegengesetzten Vorzeichen, wie man sogleich sieht, wenn man in derselben $k - \lambda$ statt k setzt. Man hat daher folgende Congruenz,

welcher alle complexen Zahlen $F(\alpha)$ genügen müssen, die sich als Normen von wirklichen complexen Zahlen in u, u_1 darstellen lassen:

$$(9.)\quad \Sigma(-1)^k\,(d_{\lambda-k}+\delta_{\lambda-k})\,C_k+(n-n_1)\,\Sigma(-1)^k\,\delta_{\lambda-k}\,d_k\equiv 0,\ \text{mod. }\lambda.$$

Um diese Congruenz in einer übersichtlicheren Form darzustellen, führe ich folgende abgekürzte Bezeichnungen der auch in dem Folgenden mehrfach wiederkehrenden Ausdrücke ein:

$$(10.)\quad \begin{aligned} mS &\equiv -d_{\lambda-1}C_1+d_{\lambda-2}C_2+d_{\lambda-4}C_4+\ldots+d_3C_{\lambda-3},\\ m_1S_1 &\equiv -\delta_{\lambda-1}C_1+\delta_{\lambda-2}C_2+\delta_{\lambda-4}C_4+\ldots+\delta_3C_{\lambda-3},\\ ms &\equiv -d_{\lambda-1}\delta_1+d_{\lambda-2}\delta_2+d_{\lambda-4}\,{}_4\delta+\ldots+d_3\delta_{\lambda-3},\quad \text{mod.}\lambda.\\ m_1s_1 &\equiv -\delta_{\lambda-1}d_1+\delta_{\lambda-2}d_2+\delta_{\lambda-4}d_4+\ldots+\delta_3d_{\lambda-3},\\ T &\equiv -(d_1+\delta_1)\,C_{\lambda-1}+(d_2+\delta_2)\,C_{\lambda-2}+(d_4+\delta_4)\,C_{\lambda-4}+\\ &\qquad +\ldots+(d_{\lambda-3}+\delta_{\lambda-3})\,C_3. \end{aligned}$$

Vermittelst dieser Zeichen stellt sich die gefundene Congruenz (9.) in folgender Weise dar:

$$(11.)\quad T-mS-m_1S_1+(n-n_1)\,(ms-m_1s_1)\equiv 0,\ \text{mod. }\lambda.$$

Es ist nun auch umgekehrt zu zeigen, wenn die Werthe der Gröfsen C_1, C_2, C_3, C_4, ... $C_{\lambda-1}$ und der Zahlen n und n_1 irgend wie gegeben sind, mit der einzigen Bedingung, dafs sie dieser Congruenz (11.) genügen, dafs man stets eine wirkliche complexe Zahl in u, u_1, $F(u, u_1)$ finden kann, welcher diese Werthe angehören. Man kann zunächst, wie oben gezeigt worden ist, immer wirkliche complexe Zahlen $F'(w)$ finden, denen die Werthe C'_1, C'_2, C'_3, ... $C'_{\lambda-1}$ angehören, wenn dieselben irgend wie so gegeben sind, dafs sie der Congruenz (5.) genügen. Ist nun $F'(w)$ eine solche passende Zahl, so ist allgemein $F'(w)+\varrho\psi(w)$ eine complexe Zahl, welche dieselben Werthe der Gröfsen C'_1, C'_2, C'_3, ... $C'_{\lambda-1}$ giebt, wo $\psi(w)$ vollständig beliebig ist; denn es ist die Norm von $F'(w)+\varrho\psi(w)$ der Norm von $F'(w)$ congruent, nach dem Modul $\lambda\varrho$. Die beliebige Zahl $\psi(w)$ kann nun immer so bestimmt werden, dafs in der complexen Zahl $F'(w)+\varrho\psi(w)$ die ersten n Coefficienten durch $u^\lambda=d(\alpha)$ theilbar sind, der $n+1$te aber nicht theilbar durch $f(\alpha)$, und dafs die ersten n_1 Coefficienten durch $u_1^\lambda=\delta(\alpha)$ theilbar sind, der n_1+1te aber nicht theilbar durch $f_1(\alpha)$. Hierdurch wird aber

$$F'(w)+\varrho\psi(w)=u^{n}\,u_1^{n_1}\,F(u, u_1),$$

und die Congruenz (5.) geht in die Congruenz (11.) über, welche letztere darum die nothwendige und hinreichende Bedingung giebt, daſs wirkliche complexe Zahlen $F(u, u_1)$ existiren, denen gegebene Werthe von C_1, C_2, $C_3, \ldots C_{\lambda-1}$, n und n_1 angehören.

Ich ziehe nun auch einen der beiden mit K und K_1 bezeichneten Charaktere mit in Betracht, welche in dem vorliegenden Falle Statt haben, wo die Determinante die beiden verschiedenen Primfaktoren $f(\alpha)$ und $f_1(\alpha)$ enthält. Der Charakter K ist definirt durch die Gleichung

$$(12.) \qquad \left(\frac{F_1(\alpha)}{f(\alpha)}\right) = \alpha^K,$$

in welcher $F_1(\alpha)$ die complexe Zahl $F(\alpha) = NF(u, u_1)$ in ihrer primären Form bezeichnet. Da nämlich die Charaktere für die Normen der idealen Zahlen in z Statt haben, von welchen festgesetzt worden ist, daſs sie stets in der primären Form genommen werden sollen, so ist in dieser Bestimmung des Charakters K die Norm der idealen Zahl in z nicht in der, gewöhnlich nicht primären Form zu nehmen, in welcher sie als Norm der wirklichen Zahl $F(u, u_1)$ erhalten wird, sondern auf die primäre Form zu bringen.

Aus der bei (2.) gegebenen Form der complexen Zahl $F(u, u_1)$, in welcher das $n+1$te Glied: $A_n\, u_1^{|n-n_1|}$ das einzige ist, welches u nicht enthält, folgt nun, daſs in der Norm $NF(u, u_1)$ das Glied $A_n^\lambda\, u^{|n-n_1|\lambda}$ das einzige sein muſs, welches u^λ nicht enthält, man hat daher die Congruenz:

$$F(\alpha) \equiv A_n^\lambda\, \delta(\alpha)^{|n-n_1|}, \quad \text{mod. } d(\alpha),$$

welche folgende Gleichung giebt:

$$(13.) \qquad \left(\frac{F(\alpha)}{d(\alpha)}\right) = \left(\frac{\delta(\alpha)}{d(\alpha)}\right)^{n-n_1}.$$

Man kann nun, weil $d(\alpha) = e(\alpha) f(\alpha)^m$ ist, die Gleichung (12.) auch in folgende Form setzen:

$$(14.) \qquad \left(\frac{F_1(\alpha)}{d(\alpha)}\right) = \alpha^{mK},$$

und erhält so, indem man die in diesen beiden Gleichungen enthaltenen Legendreschen Zeichen für das nicht primäre $F(\alpha)$ und für das zugehörige primäre $F_1(\alpha)$ nach der Formel (23.) §. 14. aufeinander zurückführt:

$$\left(\frac{\delta(\alpha)}{d(\alpha)}\right)^{n-n_1} = \alpha^{mK - d_{\lambda-1}C_1 + d_{\lambda-2}C_2 + d_{\lambda-4}C_4 + \ldots + d_3 C_{\lambda-3}}$$

und wenn man von dem bei (10.) angegebenen abgekürzten Zeichen Gebrauch macht:

$$(15.)\qquad \left(\frac{\delta(\alpha)}{d(\alpha)}\right)^{n-n_1} = \alpha^{mK+mS}.$$

Ich nehme nun die in $\delta(\alpha)$ enthaltene Primzahl $f_1(\alpha)$ primär, also auch $f_1(\alpha)^{m_1}$ primär, und drücke wieder nach der Formel (23.) §. 14. das Legendresche Zeichen der Gleichung (15.) für das nichtprimäre $\delta(\alpha)$ durch das entsprechende Zeichen für das zugehörige primäre $f_1(\alpha)^{m_1}$ aus, so ist:

$$\left(\frac{\delta(\alpha)}{d(\alpha)}\right) = \left(\frac{f_1(\alpha)}{d(\alpha)}\right)^{m_1} \alpha^{-d_{\lambda-1}\delta_1 + d_{\lambda-2}\delta_2 + d_{\lambda-4}\delta_4 + \dots + d_3\delta_{\lambda-3}}$$

und wenn von dem bei (10.) angegebenen abgekürzten Zeichen Gebrauch gemacht wird:

$$(16.)\qquad \left(\frac{\delta(\alpha)}{d(\alpha)}\right) = \left(\frac{f_1(\alpha)}{d(\alpha)}\right)^{m_1} \alpha^{ms}.$$

Weil nun $d(\alpha) = e(\alpha) f(\alpha)^m$ ist, so ist

$$\left(\frac{f_1(\alpha)}{d(\alpha)}\right) = \left(\frac{f_1(\alpha)}{f(\alpha)}\right)^m,$$

und wenn

$$\left(\frac{f_1(\alpha)}{f(\alpha)}\right) = \alpha^i$$

gesetzt wird, so erhält man aus den Gleichungen (15.) und (16.) die Congruenz

$$(17.)\qquad K + S \equiv (n - n_1)(m_1 i + s), \text{ mod. } \lambda.$$

Vermittelst der beiden Congruenzen (11.) und (17.) kann nun die Frage: ob es möglich ist für jede der $\lambda^{\mu+1}$ Werthverbindungen, welche die Charaktere $C_3, C_5, \dots C_{\lambda-1}$ und K haben können, eine ideale Zahl in z zu finden, welche sich als wirkliche complexe Zahl in u, u_1 darstellen läſst, vollständig gelöst werden; denn wenn für alle möglichen gegebenen Werthe der Charaktere $C_3, C_5, \dots C_{\lambda-1}$ und K die verfügbar bleibenden Werthe der Gröſsen $C_1, C_2, C_4, \dots C_{\lambda-3}$ und der Zahl $n - n_1$ sich so bestimmen lassen, daſs diesen beiden Congruenzen genügt wird, und auch nur unter dieser Bedingung, giebt es für alle Werthverbindungen dieser Charaktere auch wirkliche complexe Zahlen in u, u_1. Bei der groſsen Anzahl der verfügbar bleibenden Gröſsen, nämlich $\mu + 1$, mittelst deren man nur zwei Congruenzen zu

genügen hat, ist klar, dafs die Aufgabe im Allgemeinen immer lösbar sein wird, und dafs wieder nur gewisse besondere Werthe der Determinante $D(\alpha)$ Ausnahmen begründen können. Für den Zweck der gegenwärtigen Abhandlung ist es nicht erforderlich, diese Ausnahmen einzeln zu erörtern, es reicht vielmehr hin, nur den einen Fall vollständig zu untersuchen, wo von den beiden in der Determinante enthaltenen Primzahlen $f(\alpha)$ und $f_1(\alpha)$ in Beziehung auf die Einheiten die eine der ersten Art, die andere der zweiten Art angehört, uud wo die Primzahl der ersten Art $f_1(\alpha)$ Nichtrest der Primzahl der zweiten Art $f(\alpha)$ ist.

In diesem besonderen Falle hat man, weil in Beziehung auf $f(\alpha)$ und darum auch in Beziehung auf $d(\alpha)$ alle Einheiten λte Potenzreste sind:

$$d_3 \equiv 0, \quad d_5 \equiv 0, \quad \ldots d_{\lambda-2} \equiv 0, \quad d_{\lambda-1} \equiv 0, \quad \text{mod. } \lambda,$$

und darum

$$S \equiv 0 \quad \text{und} \quad s \equiv 0, \quad \text{mod. } \lambda,$$

die beiden Congruenzen (11.) und (17.) nehmen daher folgende einfachere Formen an:

$$\left.\begin{aligned} &(18.) \qquad T - m_1 S_1 - (n - n_1) m_1 s_1 \equiv 0, \\ &(19.) \qquad K - (n - n_1) m_1 i \equiv 0, \end{aligned}\right\} \text{mod. } \lambda.$$

Weil nach der Voraussetzung $f_1(\alpha)$ Nichtrest von $f(\alpha)$ ist, so ist i nicht $\equiv 0$, mod. λ, und da auch m_1 nicht durch λ theilbar ist, so folgt, dafs der Congruenz (19.) durch passende Bestimmung der Zahl $n - n_1$ immer genügt werden kann. In der Congruenz (18.) kommen nun die noch verfügbaren Gröfsen $C_1, C_2, C_4, \ldots C_{\lambda-3}$ alle nur lineär vor, sie wird also durch dieselben stets erfüllt werden können, wenn diese nicht alle aus der Congruenz dadurch verschwinden, dafs die Gröfsen, mit denen sie multiplicirt sind, alle einzeln congruent Null sind. Diese Gröfsen, mit denen sie behaftet vorkommen, sind folgende: $d_3 + \delta_3$, $d_5 + \delta_5$, $\ldots d_{\lambda-2} + \delta_{\lambda-2}$, $d_{\lambda-1} + \delta_{\lambda-1}$ oder weil $d_3, d_5, \ldots\ldots d_{\lambda-2}, d_{\lambda-1}$ alle congruent Null sind, $\delta_3, \delta_5, \ldots\ldots \delta_{\lambda-2}, \delta_{\lambda-1}$, und da $f_1(\alpha)$ nach der Voraussetzung eine Primzahl der ersten Art ist, so sind dieselben nicht alle congruent Null, es kann also auch der Congruenz (18.) immer genügt werden. Man kann also zu jeder der $\lambda^{\mu+1}$ Werthverbindungen, welche die Charaktere $C_3, C_5, \ldots C_{\lambda-1}$ und K haben können, zugehörige ideale Zahlen in z angeben, und zwar solche,

welche als wirkliche complexe Zahlen in u, u_1 darstellbar sind. Es existiren also $\lambda^{\mu+1}$ Gattungen der idealen Zahlen in z als wirklich vorhandene, und da nach dem Satze (IV.), §. 13. in dem gegenwärtigen Falle, wo die Determinante zwei verschiedene Primzahlen enthält, nicht mehr als $\lambda^{\mu+1}$ wirklich vorhanden sein können, so folgt, dafs diefs die genaue Anzahl derselben ist. Man hat demnach folgende zwei Sätze:

(III.) Wenn die Determinante zwei verschiedene Primfaktoren enthält, und zwar einen der ersten Art $f_1(\alpha)$ und einen der zweiten Art $f(\alpha)$, und wenn $f_1(\alpha)$ in der primären Form ein Nichtrest von $f(\alpha)$ ist, so ist die Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in z genau gleich $\lambda^{\mu+1}$, also genau gleich dem λten Theile aller angebbaren Gesamtcharaktere, und der Charakter K_1 ist durch die Charaktere C_3, C_5, ... $C_{\lambda-1}$ und K vollständig bestimmt.

(IV.) Unter denselben Voraussetzungen enthält jede wirklich vorhandene Gattung solche ideale Zahlen in z, welche sich als wirkliche complexe Zahlen in u, u_1 darstellen lassen.

§. 16.

Allgemeine Bestimmung der genauen Anzahl der wirklich vorhandenen Gattungen für die idealen Zahlen in z.

Die vollständige Erledignng der Frage nach der wahren Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in z, namentlich auch für diejenigen Determinanten, welche in den im vorigen Paragraphen gegebenen Sätzen Ausnahmen begründen, kann mit den daselbst angewandten Mitteln, nämlich mit Hülfe derjenigen idealen Zahlen in z, welche sich als wirkliche complexe Zahlen in w oder u, u_1, u_2 ... darstellen lassen, nicht geleistet werden; weil für gewisse Determinanten in der That solche Gattungen existiren, denen keine, als wirkliche Zahl in w oder in u, u_1, u_2 ... darstellbare, ideale Zahl in z angehört. Die wahre Anzahl der wirklich vorhandenen Gattungen ist auch in diesen Fällen immer genau gleich dem λten Theile aller angebbaren Gesamtcharaktere, nach der Methode aber, durch welche ich die Richtigkeit dieses Satzes begründet habe, sind zu dem

Beweise desselben die Reciprocitätsgesetze selbst erforderlich. Dessenungeachtet will ich diese Untersuchung hier so weit durchführen, dafs sie durch den nachher zu gebenden Beweis der Reciprocitätsgesetze vollständig abgeschlossen wird, und zwar hauptsächlich aus dem Grunde, weil der Hauptsatz, auf welchem diese Methode beruht, auch in dem Beweise der Reciprocitätsgesetze seine Anwendung finden wird. Dieser jetzt zu beweisende Satz ist folgender:

(I.) Wenn $F(\alpha)$, $F_1(\alpha)$, $F_2(\alpha)$ ... $F_{n-1}(\alpha)$ wirkliche complexe Zahlen sind, welche die eine Bedingung erfüllen, dafs das Produkt

$$F(\alpha)^m \; F_1(\alpha)^{m_1} \; F_2(\alpha)^{m_2} \; \dots\dots \; F_{n-1}(\alpha)^{m_{n-1}}$$

für ganzzahlige Werthe der Exponenten m, m_1, m_2 .... m_{n-1} nicht anders eine λte Potenz werden kann, als wenn diese Exponenten alle congruent Null sind, nach dem Modul λ, so giebt es stets unendlich viele verschiedene Primzahlen $\phi(\alpha)$, in Beziehung auf welche die Indices der complexen Zahlen $F(\alpha)$, $F_1(\alpha)$, ... $F_{n-1}(\alpha)$ beliebig gegebenen Zahlen proportional sind, nach dem Modul λ.

Um diesen Satz zu beweisen, wende ich die Methode von Hrn. Dirichlet an, durch welche derselbe den Satz bewiesen hat, dafs in jeder arithmetischen Reihe, in welcher nicht alle Glieder einen gemeinschaftlichen Faktor haben, unendlich viele Primzahlen enthalten sind. Ich setze

$$(1.) \qquad F(\alpha)^b \; F_1(\alpha)^{b_1} \; F_2(\alpha)^{b_2} \; \dots \; F_{n-1}(\alpha)^{b_{n-1}} = D(\alpha)$$

und bilde das unendliche Produkt:

$$(2.) \qquad \Pi \left(1 - \frac{\left(\frac{D(\alpha)}{\phi(\alpha)}\right)^k}{(N\phi(\alpha))^s} \right)^{-1} = L_k ,$$

in welchem das Produktzeichen Π auf alle unendlich vielen verschiedenen Primzahlen $\phi(\alpha)$ sich bezieht, mit Ausschlufs der in $\varrho D(\alpha)$ enthaltenen, welches Produkt bereits im §. 6., bei der Untersuchung der Klassenanzahl der idealen complexen Zahlen in w, seine Anwendung gefunden hat.

Der Logarithmus von L_k entwickelt giebt:

$$(3.)\qquad \log.\, L_k = \Sigma \frac{\left(\frac{D(\alpha)}{\phi(\alpha)}\right)^k}{(N\phi(\alpha))^s} + \frac{1}{2}\Sigma \frac{\left(\frac{D(\alpha)}{\phi(\alpha)}\right)^{2k}}{(N\phi(\alpha))^{2s}} + $$
$$+ \frac{1}{3}\Sigma \frac{\left(\frac{D(\alpha)}{\phi(\alpha)}\right)^{3k}}{(N\phi(\alpha))^{3s}} + \ldots\ldots$$

wo die Summenzeichen auf alle verschiedenen, nicht in $D(\alpha)$ enthaltenen Primzahlen $\phi(\alpha)$ zu beziehen sind. Alle diese Summen, mit Ausschlufs der ersten, haben die Eigenschaft, dafs sie für $s = 1$ nur endliche bestimmte Werthe haben, selbst dann, wenn $D(\alpha)$ eine λte Potenz ist, wo $\frac{D(\alpha)}{\phi(\alpha)}$ stets den Werth Eins hat, denn in den Nennern der Brüche, aus welchen sie bestehen, kommen nur die Quadrate oder Cuben oder höhere Potenzen der nichtcomplexen Primzahlen vor, und zwar jede derselben nur λ mal, weil es nicht mehr als λ conjugirte Primzahlen $\phi(\alpha)$ giebt, welche dieselbe Norm haben. Wenn daher mit $G(s)$ eine jede beliebige eindeutige Funktion von s bezeichnet wird, welche in den Grenzen $s = 1$ bis $s = \infty$ continuirlich ist, und auch für $s = 1$ einen endlichen bestimmten Werth behält, so kann die Gleichung (3.) einfacher so dargestellt werden:

$$(4.)\qquad \log.\, L_k = \Sigma \frac{\left(\frac{D(\alpha)}{\phi(\alpha)}\right)^k}{(N\phi(\alpha))^s} + G(s).$$

Wenn nun der Kürze wegen folgender, aus den in $D(\alpha)$ enthaltenen Zahlen $b, b_1, b_2, \ldots b_{n-1}$ und aus anderen n Zahlen $c, c_1, c_2, \ldots c_{n-1}$ gebildete Ausdruck:

$$(5.)\qquad bc + b_1 c_1 + b_2 c_2 + \ldots b_{n-1} c_{n-1}$$

mit C bezeichnet wird, und man multiplicirt die Gleichung (4.) mit α^{-C}, und nimmt sodann die Summe für alle Werthe des $b = 0, 1, 2, \ldots \lambda - 1$, $b_1 = 0, 1, 2, \ldots \lambda - 1$ u. s. w. so erkennt man zunächst, weil

$$\alpha^{-C}\left(\frac{D(\alpha)}{\phi(\alpha)}\right)^k = \alpha^{-bc}\left(\frac{F(\alpha)}{\phi(\alpha)}\right)^{bk} \cdot \alpha^{-b_1 c_1}\left(\frac{F_1(\alpha)}{\phi(\alpha)}\right)^{b_1 k} \ldots\ldots$$
$$\ldots\ldots \alpha^{-b_{n-1} c_{n-1}}\left(\frac{F_{n-1}(\alpha)}{\phi(\alpha)}\right)^{b_{n-1} k},$$

dafs die, in Beziehung auf die angegebenen Werthe der Zahlen $b, b_1, b_2,$

... b_{n-1} genommene Summe dieses Ausdrucks immer gleich Null wird, wenn nicht gleichzeitig

$$(6.) \quad \left(\frac{F(\alpha)}{\phi(\alpha)}\right)^k = \alpha^c\,, \quad \left(\frac{F_1(\alpha)}{\phi(\alpha)}\right)^k = \alpha^{c_1} \;\ldots\; \left(\frac{F_{n-1}(\alpha)}{\phi(\alpha)}\right)^k = \alpha^{c_{n-1}}\,,$$

daſs aber, wenn diese Gleichungen zugleich Statt haben, diese Summe gleich λ^n ist. Es folgt dieſs unmittelbar daraus, daſs die Legendreschen Zeichen nur Potenzen von α sind, und daſs $1 + \alpha^r + \alpha^{2r} + \ldots + \alpha^{(\lambda-1)r}$ gleich Null ist, wenn r nicht durch λ theilbar ist, aber gleich λ, wenn r durch λ theilbar ist. Man hat daher:

$$(7.) \qquad S\,\alpha^{-c} \log. L_k = \lambda^n \Sigma \frac{1}{(N\phi(\alpha))^s} + G(s),$$

wo das Summenzeichen S auf alle Werthe der in C und L_k enthaltenen Zahlen $b = 0, 1, 2, \ldots \lambda - 1$, $b_1 = 0, 1, 2, \ldots \lambda - 1$ u. s. w. sich bezieht, das Summenzeichen Σ aber auf alle diejenigen Primzahlen $\phi(\alpha)$, welche den bei (6.) gegebenen Bedingungen genügen, und wo $G(s)$ eine Funktion von s von derselben Beschaffenheit ist, als die oben mit demselben Zeichen belegte. Endlich gebe ich noch der unbestimmten Zahl k die Werthe 1, 2, 3 ... $\lambda - 1$ und summire, so wird:

$$(8.) \qquad S\,\alpha^{-c} \log. (L_1, L_2, L_3 \ldots L_{\lambda-1}) = \lambda^n \Sigma \frac{1}{(N\phi(\alpha))^s} + G(s),$$

wo das Summenzeichen Σ auf alle diejenigen complexen Primzahlen $\psi(\alpha)$ sich erstreckt, welche den Bedingungen (6.), für irgend welche Werthe des $k = 1, 2, 3, \ldots \lambda - 1$ genügen.

Das Produkt $L_1\, L_2\, L_3 \ldots L_{\lambda-1}$ ist, wie im §. 6. gezeigt worden ist, für den Werth $s = 1$ ein Faktor der Klassenanzahl aller idealen Zahlen in w der Determinante $D(\alpha)$, welche den bei (1.) angegebenen Werth hat. Dieses Produkt ist daher für $s = 1$ immer endlich, sobald $D(\alpha)$ die einzige Bedingung erfüllt, welche bei der Entwickelung dieser Klassenanzahl gemacht worden ist, nämlich, daſs die Determinante nicht eine vollständige λte Potenz sei, in welchem Falle von complexen Zahlen in w gar nicht die Rede sein kann. Nach der Voraussetzung des Satzes ist aber $D(\alpha)$ niemals eine λte Potenz, wenn nicht alle Exponenten $b, b_1, b_2, \ldots b_{n-1}$ einzeln congruent Null sind, nach dem Modul λ; darum ist das eine Glied der Summe S, für welches $b = 0$, $b_1 = 0$, $b_2 = 0$, $b_{n-1} = 0$ ist, das einzige, welches für $s = 1$ nicht einen endlichen Werth behalten muſs. Wirft man nun alle

die Glieder dieser Summe, von denen fest steht, daſs sie für $s = 1$ endliche Werthe behalten, auf die andere Seite der Gleichung und vereinigt sie dort mit den durch $G(s)$ bezeichneten Theilen, so hat man, weil das unendliche Produkt L_k für $D(\alpha) = 1$ dasselbe ist als L_0:

$$(9.) \qquad (\lambda - 1) \log. L_0 = \lambda^s \, \Sigma \frac{1}{(N\phi(\alpha))^s} + G(s).$$

Läſst man nun s bis zur Gränze $s = 1$ abnehmen, so wird L_0 unendlich groſs, wie im §. 6. gezeigt worden ist, $G(s)$ aber bleibt endlich; darum muſs die Summe Σ, welche sich auf die Primzahlen $\phi(\alpha)$ bezieht unendlich groſs werden, es muſs also unendlich viele Primzahlen $\phi(\alpha)$ geben, welche den bei (6.) angegebenen Bedingungen, für gewisse Werthe des $k = 1, 2, 3, \ldots \lambda - 1$ genügen. Setzt man diese Bedingungen, indem man anstatt der Legendreschen Zeichen die Indices anwendet, welche sich auf die Primzahl $\phi(\alpha)$ als Modul beziehen, in die Form

$$(10.) \qquad k \,\text{Ind.}\, F(\alpha) \equiv c, \; k \,\text{Ind.}\, F_1(\alpha) \equiv c_1, \ldots k \,\text{Ind.}\, F_{n-1}(\alpha) \equiv c_{n-1}, \; \text{mod}\, \lambda.$$

so hat man die Indices dieser complexen Zahlen $F(\alpha)$, $F_1(\alpha) \ldots . F_{n-1}(\alpha)$ proportional den beliebig gegebenen Zahlen $c, c_1, \ldots c_{n-1}$, nach dem Modul λ, was zu beweisen war.

Um den gefundenen Satz auf die Frage wegen der wahren Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in z anzuwenden, nehme ich für die Zahlen $F(\alpha)$, $F_1(\alpha)$, $F_2(\alpha) \ldots F_{n-1}(\alpha)$ folgende $\mu + r$:

$$(11.) \qquad E_1(\alpha), E_2(\alpha), \ldots E_{\mu-1}(\alpha), f(\alpha)^m, f_1(\alpha)^{m_1}, \ldots f_{r-1}(\alpha)^{m_{r-1}}$$

wo $E_n(\alpha)$ folgende zusammengesetzte Kreistheilungseinheit bezeichnet:

$$(12.) \qquad E_n(\alpha) = e(\alpha)\, e(\alpha^{\gamma})^{\gamma^{-2n}}\, e(\alpha^{\gamma^2})^{\gamma^{-4n}} \ldots e(\alpha^{\gamma^{\mu-1}})^{\gamma^{-2(\mu-1)n}},$$

von welcher ich in der Abhandlung über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen bewiesen habe, daſs ihr Index in Beziehung auf die Primzahl $\phi(\alpha)$ folgenden Werth hat:

$$(13.) \qquad \text{Ind.}\, E_n(\alpha) \equiv (-1)^n (\gamma^{2n} - 1) \frac{B_n}{4n} \frac{d_0^{\lambda-2n} l\phi(e^v)}{dv^{\lambda-2n}}, \; \text{mod.}\, \lambda.$$

wenn B_n die $n$te Bernoullische Zahl ist, und γ die in $E_n(\alpha)$ enthaltene, primitive Wurzel der Primzahl λ; wo ferner $f(\alpha)$, $f_1(\alpha)$, $\ldots f_{r-1}(\alpha)$ verschie-

dene Primzahlen sind, welche alle primär genommen werden sollen, und die Exponenten $m, m_1, \dots m_{r-1}$ so beschaffen, daſs diese Potenzen wirklich werden, wenn die complexen Zahlen selbst ideal sind. Diese $\mu + r$ wirklichen complexen Zahlen erfüllen die in dem Satze ausgesprochene Bedingung, daſs ein Produkt von Potenzen derselben nicht eine λte Potenz sein kann, ohne daſs die Exponenten der Potenzen alle einzeln durch λ theilbar sind. Wenn nämlich das Produkt:

$$(14.)\qquad \alpha^{b}\, E_1(\alpha)^{b_1}\, E_2(\alpha)^{b_2} \dots E_{\mu-1}(\alpha)^{b_{\mu-1}}\, f(\alpha)^{b_\mu m}\, f_1(\alpha)^{b_{\mu+1} m_1} \dots$$
$$\dots f_{r-1}(\alpha)^{b_{\mu+r-1} m_{r-1}}$$

eine λte Potenz sein soll, so müssen zunächst, weil $f(\alpha), f_1(\alpha), \dots f_{r-1}(\alpha)$ verschiedene Primzahlen sind, $b_\mu, b_{\mu+1}, \dots b_{\mu+r-1}$ alle Vielfache von λ sein, weil $m, m_1 \dots m_{r-1}$ nicht durch λ theilbar sind; ferner muſs b ein Vielfaches von λ sein, weil die λte Potenz einer wirklichen complexen Zahl in α nothwendig einer nichtcomplexen Zahl congruent ist nach dem Modul λ und weil, wenn b nicht durch λ theilbar ist, dieses Produkt selbst nicht für den Modul ϱ^2 einer nichtcomplexen Zahl congruent sein kann. Es bleibt also nur noch zu zeigen, daſs auch das Produkt

$$E_1(\alpha)^{b_1}\, E_2(\alpha)^{b_2} \dots E_{\mu-1}(\alpha)^{b_{\mu-1}}$$

nicht eine λte Potenz sein kann, ohne daſs $b_1, b_2, \dots b_{\mu-1}$ alle durch λ theilbar sind. Dieses wird am leichtesten mit Hülfe des in der genannten Abhandlung pag. 134. gegebenen Ausdrucks des Logarithmus der Einheit $E_n(\alpha)$ gezeigt, nach welchem

$$(15.)\qquad l\left(\frac{E_n(\alpha)}{E(1)}\right) \equiv -(-1)^n\,(\gamma^{2n}-1)\,\frac{B_n}{4n}\,\chi_{2n}(\alpha),\ \text{mod. } \lambda,$$
$$\chi_{2n}(\alpha) = \alpha + \gamma^{-2n}\,\alpha^{\gamma} + \gamma^{-4n}\,\alpha^{\gamma^2} + \dots + \gamma^{-2(\lambda-2)n}\,\alpha^{\gamma^{\lambda-2}}.$$

Vermöge dieses Ausdrucks wird der Logarithmus des obigen Produkts congruent:

$$(16.)\qquad -b_1\,\beta_1\,\chi_2(\alpha) - b_2\,\beta_2\,\chi_4(\alpha) - \dots - b_{\mu-1}\,\beta_{\mu-1}\,\chi_{2\mu-2}(\alpha),$$

nach dem Modul λ, wo der Kürze wegen

$$(-1)^n (\gamma^{2n} - 1) \frac{B_n}{4n} = \beta_n$$

gesetzt ist. Dieser Ausdruck des Logarithmus des Produkts mufs congruent Null sein, wenn das Produkt eine λte Potenz ist, welches nicht anders geschehen kann, als dafs alle Glieder einzeln congruent Null sind, also $b_1\beta_1 \equiv 0$, $b_2\beta_2 \equiv 0$, $b_{\mu-1}\beta_{\mu-1} \equiv 0$, und weil keine der Zahlen β_1, β_2, ... $\beta_{\mu-1}$ durch λ theilbar ist, so müssen die Zahlen b_1, b_2, ... $b_{\mu-1}$ alle durch λ theilbar sein.

Da also die bei (11.) angenommenen complexen Zahlen den Bedingungen des Satzes (I.) entsprechen, so folgt, dafs es unendlich viele Primzahlen $\phi(\alpha)$ giebt, für welche

$$\begin{gathered} k \text{ Ind. } (\alpha) \equiv -C_{\lambda-1}, \; k \text{ Ind. } E_1(\alpha) \equiv \beta_1 C_{\lambda-2}, \; k \text{ Ind. } E_2(\alpha) \equiv \beta_2 C_{\lambda-4} \\ \ldots k \text{ Ind. } E_{\mu-1}(\alpha) \equiv \beta_{\mu-1} C_3, \; k \text{ Ind. } f(\alpha)^m \equiv mK, \\ \ldots k \text{ Ind. } f_{\mu-1}(\alpha)^{m_{r-1}} \equiv m_{r-1} K_{r-1} \end{gathered} \tag{17.}$$

ist, für alle beliebig gegebenen Werthe der Zahlen $C_{\lambda-1}$, $C_{\lambda-2}$, $C_{\lambda-4}$ ... C_3, K, K_1, ... K_{r-1}. Diese Congruenzen können vermöge des bei (13.) gegebenen Ausdrucks des Index der Einheit $E_n(\alpha)$, und vermittelst des Legendreschen Zeichens auch so dargestellt werden:

$$\begin{gathered} k \frac{1 - N\phi(\alpha)}{\lambda} \equiv C_{\lambda-1}, \quad k \frac{d_0^{\lambda-2} l \phi(e^v)}{dv^{\lambda-2}} \equiv C_{\lambda-2}, \\ k \frac{d_0^{\lambda-4} l \phi(e^v)}{dv^{\lambda-4}} \equiv C_{\lambda-4} \; \ldots\ldots \quad k \frac{d_0^3 l \phi(e^v)}{dv^3} \equiv C_3, \\ \left(\frac{f(\alpha)}{\phi(\alpha)}\right)^k \equiv a^K \; \ldots\ldots \left(\frac{f_{r-1}(\alpha)}{\phi(\alpha)}\right)^k \equiv a^{K_{r-1}}. \end{gathered} \tag{18.}$$

Es ist nun die Bedingung einzuführen, dafs die Primzahl $\phi(\alpha)$ die Norm einer idealen Primzahl $\phi(z)$ der Determinante

$$D(\alpha) = \varepsilon(\alpha) f(\alpha)^m f_1(\alpha)^{m_1} \ldots\ldots f_{r-1}(\alpha)^{m_{r-1}}$$

ist, welche darin besteht, dafs $\left(\frac{D(\alpha)}{\phi(\alpha)}\right) = 1$ sei. Setzt man der Kürze wegen:

$$\frac{d_0^n l \varepsilon(e^v)}{dv^n} = \varepsilon_n,$$

so hat man zunächst nach der §. 14., bei (25.) gegebenen Formel,

$$\left(\frac{\varepsilon(\alpha)}{\phi(\alpha)}\right) = \alpha^{-\varepsilon_1 C_{\lambda-1} + \varepsilon_2 C_{\lambda-2} + \varepsilon_4 C_{\lambda-4} + \ldots + \varepsilon_{\lambda-3} C_3},$$

die Bedingung $\left(\frac{D(\alpha)}{\phi(\alpha)}\right) = 1$ giebt daher:

$$\begin{aligned}(19.)\qquad & -\varepsilon_1 C_{\lambda-1} + \varepsilon_2 C_{\lambda-2} + \varepsilon_4 C_{\lambda-4} + \ldots + \varepsilon_{\lambda-3} C_3 + mK + m_1 K_1 \\ & \qquad + \ldots + m_{r-1} K_{r-1} \equiv 0, \quad \text{mod. } \lambda.\end{aligned}$$

Vermöge dieser Congruenz wird eine der $\mu + r$ Gröfsen $C_{\lambda-1}$, $C_{\lambda-2}$, ... C_3, $K, K_1, \ldots K_{r-1}$, als welche die letzte K_{r-1} genommen werden kann, durch die übrigen $\mu + r - 1$ bestimmt, deren jede einzelne alle Werthe 0, 1, 2, ... $\lambda - 1$ annehmen kann, so dafs im Ganzen $\lambda^{\mu+r-1}$ Werthverbindungen der Gröfsen $C_{\lambda-1}$, $C_{\lambda-2}$, ... C_3, K, K_1, ... K_{r-1} bestehen, für welche $\phi(\alpha)$ die Norm einer idealen Zahl $\phi(z)$ ist.

Wenn nun, wie in dem Folgenden bewiesen werden wird, zwischen je zwei complexen primären Primzahlen $f(\alpha)$ und $\phi(\alpha)$ das Reciprocitätsgesetz

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right)$$

besteht, so kann man demgemäfs statt

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right),\ \left(\frac{f_1(\alpha)}{\phi(\alpha)}\right),\ \ldots\ \left(\frac{f_{r-1}(\alpha)}{\phi(\alpha)}\right)$$

die Ausdrücke

$$\left(\frac{\phi(\alpha)}{f(\alpha)}\right),\ \left(\frac{\phi(\alpha)}{f_1(\alpha)}\right),\ \left(\frac{\phi(\alpha)}{f_{r-1}(\alpha)}\right)$$

nehmen und die Congruenzen folgendermaafsen darstellen:

$$\begin{aligned}(20.)\qquad & \frac{1 - N\phi(\alpha)^k}{\lambda} \equiv C_{\lambda-1},\ \frac{d_0^{\lambda-2}\, l\phi(e^v)^k}{dv^{\lambda-2}} \equiv C_{\lambda-2},\ \frac{d_0^{\lambda-4}\, l\phi(e^v)^k}{dv^{\lambda-4}} \equiv C_{\lambda-4} \ldots \\ & \frac{d_0^3\, l\phi(e^v)^k}{dv^3} \equiv C_3,\ \left(\frac{\phi(\alpha)^k}{f(\alpha)}\right) = \alpha^K,\ \ldots\ \left(\frac{\phi(\alpha)^k}{f_{r-1}(\alpha)}\right) = \alpha^{K_{r-1}}.\end{aligned}$$

Die ideale Zahl $\phi(z)^k$, deren Norm gleich $\phi(\alpha)^k$, ist also eine solche, welche die Charaktere $C_{\lambda-1}$, $C_{\lambda-2}$, $C_{\lambda-4}$, ... C_3, K, K_1, ... K_{r-1} hat, welche der einzigen Bedingung (19.) unterworfen sind, und wie auch die Werthe dieser Charaktere gewählt werden mögen, wenn sie nur der in der Congruenz (19.) gegebenen Bedingung genügen, so giebt es stets ideale Zahlen

$\phi(z)^t$, welchen diese Charaktere zukommen. Die Anzahl der angebbaren Gesamtcharaktere, welche gleich $\lambda^{\mu+r}$ ist, weil jeder der $\mu+r$ Charaktere die λ Werthe $0, 1, 2, \ldots \lambda-1$ haben kann, wird durch die Congruenz (19.) genau auf den λten Theil eingeschränkt, diese $\lambda^{\mu+r-1}$ Gesamtchararaktere geben aber ebensoviele wirklich vorhandene Gattungen, weil jedem derselben ideale Zahlen in z angehören.

Hiermit ist, unter der Voraussetzung, dafs unter je zwei primären complexen Primzahlen $f(\alpha)$ und $\phi(\alpha)$ das Reciprocitätsgesetz $\left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right)$ gültig ist, der Satz bewiesen:

(II.) **Die Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in z ist genau gleich dem λten Theile aller angebbaren Gesamtcharaktere.**

§. 17.

Beweis der allgemeinen Reciprocitätsgesetze.

In dem Beweise der allgemeinen Reciprocitätsgesetze zwischen je zwei complexen Primzahlen in α, welcher sich auf die in dem Vorhergehenden entwickelte Theorie der complexen Zahlen in z, und namentlich auf die Eintheilung der idealen Zahlen dieser Theorie in die Gattungen stützt, sind diejenigen complexen Primzahlen in α, in Beziehung auf welche alle Einheiten λte Potenzreste sind, die als complexe Primzahlen der zweiten Art bezeichneten, von denen, welche diese besondere Eigenschaft nicht haben, den complexen Primzahlen der ersten Art, zu unterscheiden und namentlich folgende drei Fälle besonders zu behandeln: erstens der Fall, wo beide zu vergleichenden complexen Primzahlen der ersten Art angehören, zweitens, wo eine der ersten Art, die andere der zweiten Art angehört und drittens, wo beide der zweiten Art angehören.

Für den ersten dieser drei Fälle reicht es hin, nur solche complexe Zahlen in z anzuwenden, deren Determinante nicht mehr als einen idealen Primfaktor enthält. Es sei also:

$$D(\alpha) = e(\alpha)f(\alpha)^m,$$

$f(\alpha)$ eine complexe Primzahl der ersten Art, welche primär angenommen

werden soll, m ein nicht durch λ theilbarer Exponent, welcher bewirkt, dafs $f(\alpha)^m$ wirklich ist, wenn $f(\alpha)$ selbst ideal sein sollte, und $e(\alpha)$ eine beliebige Einheit, welche jedoch durch die Bedingung, dafs $D(\alpha) - 1$ durch ϱ, aber nicht durch ϱ^2 theilbar sein soll, einer gewissen Beschränkung unterworfen ist.

Unter diesen Voraussetzungen ist von den $\mu + 1$ Charakteren C_3, C_5, ... $C_{\lambda-1}$ und K, welche überhaupt Statt haben, der letzte durch die übrigen vollständig bestimmt, in der Art, dafs alle idealen Zahlen in z, welche dieselben Werthe der Charaktere C_3, C_5, ... $C_{\lambda-1}$ haben, auch denselben Werth des Charakters K haben müssen. (Satz (I.) §. 16.). Wenn ferner $\phi(z)$ irgend eine ideale Primzahl in z ist, so giebt es stets eine wirkliche complexe Zahl in w, $F(w)$, welche als ideale Zahl in z betrachtet, dieselben Werthe der Charaktere C_3, C_5, ... $C_{\lambda-1}$ hat, als $\phi(z)$, (Satz (II.) §. 16.), und welche darum auch denselben Werth des letzten Charakters K haben mufs, als diese. Wird nun die Norm der idealen Primzahl $\phi(z)$ mit $\phi(\alpha)$ bezeichnet, wo $\phi(\alpha)$ nach der allgemeinen Festsetzung über die Normen der idealen Zahlen in z primär ist; wird ferner die Norm der wirklichen complexen Zahl $F(w)$ mit $F(\alpha)$ bezeichnet, und dieselbe in der primären Form genommen durch $F_1(\alpha)$, so hat man:

$$(1.)\qquad \left(\frac{F_1(\alpha)}{f(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right) = \alpha^K,$$

oder, was nach der §. 14. gegebenen Definition dieses Legendreschen Zeichens für zusammengesetzte Moduln dasselbe ist:

$$(2.)\qquad \left(\frac{F_1(\alpha)}{D(\alpha)}\right) = \alpha^{mK}.$$

Nimmt man nun

$$F(w) = A + A_1 w + A_2 w^2 + \ldots\ldots + A_{\lambda-1} w^{\lambda-1},$$

und entwickelt die Norm von $F(w)$, so ist A^λ das einzige Glied dieser Norm, welches w^λ nicht enthält, man hat also

$$NF(w) = F(\alpha) \equiv A^\lambda, \quad \text{mod. } D(\alpha),$$

oder was dasselbe ist:

$$(3.)\qquad \left(\frac{F(\alpha)}{D(\alpha)}\right) = 1.$$

Drückt man nun nach Formel (23.), §. 14. das Legendresche Zeichen für das nicht primäre $F(\alpha)$ durch das entsprechende Zeichen für das primäre $F_1(\alpha)$ aus, so hat man

$$\left(\frac{F(\alpha)}{D(\alpha)}\right) = \left(\frac{F_1(\alpha)}{D(\alpha)}\right) \alpha^{-C_1 D_{\lambda-1} + C_2 D_{\lambda-2} + C_4 D_{\lambda-4} + \ldots + C_{\lambda-3} D_3},$$

also vermöge der Gleichungen (2.) und (3.):

$$(4.) \quad mK - C_1 D_{\lambda-1} + C_2 D_{\lambda-2} + C_4 D_{\lambda-4} + \ldots + C_{\lambda-3} D_3 \equiv 0, \text{ mod. } \lambda.$$

Ferner hat man nach derselben Formel (23.), §. 14, weil $f(\alpha)^m$ die complexe Zahl $D(\alpha)$ in ihrer primären Form darstellt:

$$\left(\frac{D(\alpha)}{\phi(\alpha)}\right) = \left(\frac{f(\alpha)}{\phi(\alpha)}\right)^m \alpha^{-D_1 C_{\lambda-1} + D_2 C_{\lambda-2} + C_4 D_{\lambda-4} + \ldots + D_{\lambda-3} C_3}.$$

Setzt man nun

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \alpha^{K'}$$

und beachtet, dafs $\phi(\alpha)$ als Norm einer idealen Zahl in z der Determinante $D(\alpha)$ der Bedingung

$$(5.) \qquad \left(\frac{D(\alpha)}{\phi(\alpha)}\right) = 1$$

genügen mufs, so hat man

$$(6.) \quad mK' - D_1 C_{\lambda-1} + D_2 C_{\lambda-2} + D_4 C_{\lambda-4} + \ldots + D_{\lambda-3} C_3 \equiv 0, \text{ mod. } \lambda.$$

Verbindet man nun die beiden Congruenzen (4.) und (6.) mit der Congruenz

$$(7.) \quad D_{\lambda-1} C_1 - D_{\lambda-2} C_2 + D_{\lambda-3} C_3 - D_{\lambda-4} C_4 + \ldots + D_1 C_{\lambda-1} \equiv 0, \text{ mod. } \lambda,$$

welche nach dem Satze (I.) §. 14. Statt haben mufs, weil $F(\alpha)$ die Norm der wirklichen complexen Zahl $F(w)$ ist, so erhält man:

$$mK \equiv mK', \text{ mod. } \lambda,$$

und weil m nicht durch λ theilbar ist:

$$K \equiv K', \text{ mod. } \lambda,$$

also

$$(8.)\qquad \left(\frac{\phi(\alpha)}{f(\alpha)}\right)=\left(\frac{f(\alpha)}{\phi(\alpha)}\right).$$

Diese Gleichung giebt das Reciprocitätsgesetz unter den beiden primären Primzahlen $f(\alpha)$ und $\phi(\alpha)$, deren erste eine complexe Primzahl der ersten Art ist, und die andere $\phi(\alpha)$ eine Primzahl, welche der einen in der Gleichung (5.) enthaltenen Bedingung unterworfen ist, daſs

$$(9.)\qquad \left(\frac{e(\alpha)}{\phi(\alpha)}\right)\left(\frac{f(\alpha)}{\phi(\alpha)}\right)^m=1$$

sein muſs.

Wenn nun $f(\alpha)$ ebenfalls eine complexe Primzahl der ersten Art ist, also Einheiten $e(\alpha)$ existiren, für welche $\left(\frac{e(\alpha)}{\phi(\alpha)}\right)$ nicht gleich Eins ist, so kann man, welchen Werth auch $\left(\frac{f(\alpha)}{\phi(\alpha)}\right)$ habe, die Einheit $e(\alpha)$ in der Regel so wählen, daſs die Bedingung (9.) erfüllt wird, woraus folgt, daſs in der Reciprocitätsgleichung (8.) die Primzahl $\phi(\alpha)$ eine jede primäre Primzahl der ersten Art darstellt. In einem ganz besonderen Falle jedoch wird durch die Bedingung, welcher die Determinante $D(\alpha)$ unterworfen ist, daſs $D(\alpha)-1$ durch ϱ aber nicht durch ϱ^2 theilbar sein soll, eine Ausnahme begründet. Der primäre Faktor der Determinante: $f(\alpha)^n$ hat als solcher die Eigenschaft einer nichtcomplexen Zahl congruent zu sein, nach dem Modul ϱ^2; ferner, wenn die Einheit $e(\alpha)$ in die Form $\alpha^k\varepsilon(\alpha)$ gesetzt wird, wo $\varepsilon(\alpha)$ eine, nur die zweigliedrigen Perioden $\alpha+\alpha^{-1}$, $\alpha^2+\alpha^{-2}$, ... enthaltende Einheit ist, welche Form einer jeden Einheit in α gegeben werden kann, so hat auch $\varepsilon(\alpha)$ die Eigenschaft, einer nichtcomplexen Zahl congruent zu sein, nach dem Modul ϱ^2; da aber $D(\alpha)$ diese Eigenschaft nicht haben darf, so folgt, daſs α^k dieselbe Eigenschaft nicht haben darf. Es ist aber $\alpha^k\equiv 1-k\varrho$, mod. ϱ^2, woraus folgt, daſs k nicht durch ϱ theilbar, oder was dasselbe ist, k nicht gleich Null sein darf. Wenn nun die Primzahl $\phi(\alpha)$ die ganz besondere Eigenschaft hat, daſs für dieselbe alle aus den zweigliedrigen Perioden gebildeten Einheiten $\varepsilon(\alpha)$ λte Potenzreste sind, und wenn zugleich auch $f(\alpha)$ ein λter Potenzrest von $\phi(\alpha)$ ist, so ist die Bedingung (8.) nicht zu befriedigen, weil in $e(\alpha)=\alpha^k\varepsilon(\alpha)$ die Zahl k nicht gleich Null sein darf, es folgt aber auch, daſs dieſs der einzige Ausnahmefall ist. Es ist indessen leicht auch für diese besonderen Primzahlen $\phi(\alpha)$ die Gültigkeit der Reciprocitätsgleichung (8.) zu erschlieſsen. Weil nämlich dieser Ausnahmefall niemals eintritt, sobald

$f(\alpha)$ ein Nichtrest von $\phi(\alpha)$ ist, so zeigt die Gleichung (8.) zunächst, daſs, wenn eine der beiden Primzahlen der ersten Art $f(\alpha)$ und $\phi(\alpha)$ ein Nichtrest der anderen ist, auch diese andere Nichtrest der ersten sein muſs, und hieraus folgt sodann, daſs wenn die eine Rest der anderen ist, auch die andere Rest der ersten sein muſs; denn wäre die zweite ein Nichtrest der ersten, so müsste auch die erste ein Nichtrest der zweiten sein. Die Beschränkung der Determinante, daſs $D(\alpha)-1$ nicht durch ϱ^2 theilbar sein darf, begründet also keine Ausnahme in der Allgemeingültigkeit des Reciprocitätsgesetzes (8.) für je zwei beliebige complexe Primzahlen der ersten Art, und man hat das Resultat:

(I.) Wenn $f(\alpha)$ und $\phi(\alpha)$ zwei primäre complexe Primzahlen der ersten Art sind, so besteht unter ihnen das Reciprocitätsgesetz:

$$\left(\frac{\phi(\alpha)}{f(\alpha)}\right)=\left(\frac{f(\alpha)}{\phi(\alpha)}\right).$$

Wenn nun zweitens die Primzahl $\phi(\alpha)$ in der Gleichung (8.) eine complexe Primzahl der zweiten Art ist, für welche alle Einheiten λte Potenzreste sind, so folgt aus der Gleichung (9.), daſs $\phi(\alpha)$ die Bedingung $\left(\frac{f(\alpha)}{\phi(\alpha)}\right)=1$ erfüllen muſs, und daſs, wenn diese Bedingung erfüllt ist, die Reciprocitätsgleichung (8.) Statt hat. Man hat also folgenden Satz:

(II.) Wenn eine primäre complexe Primzahl der ersten Art, $f(\alpha)$, ein λter Potenzrest einer primären complexen Primzahl der zweiten Art, $\phi(\alpha)$ ist, so ist auch $\phi(\alpha)$ ein λter Potenzrest von $f(\alpha)$.

Daſs die Umkehrung dieses Satzes ebenfalls richtig ist, kann aus dem Vorhergehenden noch nicht erschlossen werden.

Um nun die Reciprocitätsgesetze auch für die Fälle, wo von den beiden zu vergleichenden Primzahlen die eine der ersten Art, die andere der zweiten Art angehört, und wo beide der zweiten Art angehören, vollständig zu entwickeln, wende ich complexe Zahlen in z an, deren Determinante zwei verschiedene Primfaktoren $f(\alpha)$ und $f_1(\alpha)$ enthält, für welche also

$$D(\alpha)=e(\alpha)f(\alpha)^{m}\cdot e_1(\alpha)f_1(\alpha)^{m_1}$$

ist. Es sollen auch hier $f(\alpha)$ und $f_1(\alpha)$ als primär angenommen, und m und

m_1 so gewählt werden, dafs $f(\alpha)^m$ und $f_1(\alpha)^{m_1}$ wirklich werden, wenn $f(\alpha)$ oder $f_1(\alpha)$ ideal sind; ferner soll, entsprechend den Voraussetzungen des Satzes (III), §. 15. festgesetzt werden, dafs $f(\alpha)$ eine Primzahl der zweiten Art, $f_1(\alpha)$ aber eine Primzahl der ersten Art, und dafs $f_1(\alpha)$ Nichtrest von $f(\alpha)$ sei.

Unter diesen Voraussetzungen findet nach dem Satze (IV.) §. 15. unter den Charakteren C_3, C_5, ... $C_{\lambda-1}$, K und K_1 einer jeden idealen Zahl $\phi(z)$ die Beziehung Statt, dafs der Charakter K_1 durch die übrigen Charaktere vollständig bestimmt ist, in der Art, dafs alle idealen Zahlen in z, welche dieselben Werthe der Charaktere C_3, C_5, ... $C_{\lambda-1}$ und K haben, auch denselben Werth des Charakters K_1 haben müssen. Es giebt auch zu jeder idealen Zahl $\phi(z)$ eine wirkliche complexe Zahl $F(u, u_1)$, welche als ideale Zahl in z betrachtet vollständig dieselben Werthe der Charaktere hat, als $\phi(z)$. Wenn nun wieder $\phi(z)$ als ideale Primzahl angenommen wird, und $\phi(\alpha)$ die Norm derselben, also primär ist; wenn ferner $F(\alpha)$ die Norm von $F(u, u_1)$ bezeichnet und $F_1(\alpha)$ die primäre Form der Zahl $F(\alpha)$, und wenn auch die übrigen im §. 15. festgesetzten Bezeichnungen beibehalten werden, so hat man:

$$\left(\frac{F_1(\alpha)}{f(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right) = \alpha^K, \tag{10.}$$

$$\left(\frac{F_1(\alpha)}{f_1(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f_1(\alpha)}\right) = \alpha^{K_1}. \tag{11.}$$

Aus dem Ausdrucke der complexen Zahl $F(u, u_1)$ folgt ferner für die Norm derselben $F(\alpha)$, aufser der schon im §. 15. entwickelten Gleichung:

$$\left(\frac{F(\alpha)}{f(\alpha)}\right) = \left(\frac{\delta(\alpha)}{f(\alpha)}\right)^{n-n_1}, \tag{12.}$$

ebenso auch die Gleichung:

$$\left(\frac{F(\alpha)}{f_1(\alpha)}\right) = \left(\frac{d(\alpha)}{f_1(\alpha)}\right)^{n_1-n}. \tag{13.}$$

Wenn nun nach der schon mehrmals benutzten Formel (23.), §. 14. die in diesen beiden Gleichungen vorkommenden Legendreschen Zeichen für die nichtprimären Zahlen $F(\alpha)$, $\delta(\alpha)$ und $d(\alpha)$ durch die entsprechenden für die primären Zahlen $F_1(\alpha)$, $f_1(\alpha)^{m_1}$ und $f(\alpha)^m$ ausgedrückt werden, und

$$\left(\frac{f_1(\alpha)}{f(\alpha)}\right) = \alpha^i, \quad \left(\frac{f(\alpha)}{f_1(\alpha)}\right) = \alpha^{i'}$$

gesetzt wird, so erhält man die beiden Congruenzen:

$$\begin{aligned} &(14.) \quad K \equiv (n - n_1)\, m_1 i, \\ &(15.) \quad K_1 + S_1 \equiv (n_1 - n)\,(m i' + s_1), \end{aligned} \quad \text{mod. } \lambda,$$

deren erstere schon im §. 15. hergeleitet worden ist.

Aus der Bedingung, dafs $\phi(z)$ ein idealer Primfaktor von $\phi(\alpha)$ ist, hat man ferner

$$\left(\frac{D(\alpha)}{\phi(\alpha)}\right) = \left(\frac{e(\alpha)\, e_1(\alpha)}{\phi(\alpha)}\right) \cdot \left(\frac{f(\alpha)}{\phi(\alpha)}\right)^m \cdot \left(\frac{f_1(\alpha)}{\phi(\alpha)}\right)^{m_1} = 1,$$

und wenn man das Legendresche Zeichen für die nichtprimäre Zahl $D(\alpha)$ durch das entsprechende für die primäre Zahl $f(\alpha)^m f_1(\alpha)^{m_1}$ ausdrückt, und der Kürze wegen

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \alpha^{K'}, \quad \left(\frac{f_1(\alpha)}{\phi(\alpha)}\right) = \alpha^{K'_1}$$

setzt, so erhält man aus der Bedingung, dafs $D(\alpha)$ Rest von $\phi(\alpha)$ ist, die Congruenz:

$$(16.) \quad T + mK' + m_1 K'_1 \equiv 0, \quad \text{mod. } \lambda.$$

Endlich, weil $F(\alpha)$ die Norm der wirklichen complexen Zahl $F(u, u_1)$ ist, hat man noch die §. 15, bei (18.) entwickelte Congruenz:

$$(17.) \quad T - m_1 S_1 - (n - n_1)\, m_1 s_1 \equiv 0, \quad \text{mod. } \lambda.$$

Aus den vier Congruenzen (14.), (15.), (16.) und (17.) erhält man nun durch Elimination der drei Gröfsen T, S_1 und $n - n_1$, durch welche s_1 von selbst mit weggeht, die Congruenz:

$$(18.) \quad m(iK' - i'K) + m_1 i(K'_1 - K_1) \equiv 0, \quad \text{mod. } \lambda,$$

aus welcher das Reciprocitätsgesetz für die beiden Fälle: erstens, wo eine der beiden Zahlen $f(\alpha)$ und $\phi(\alpha)$ der ersten Art, die andere der zweiten Art angehört, und zweitens, wo beide der zweiten Art angehören, entwickelt werden soll.

Ich nehme zuerst $\phi(\alpha)$ als eine Primzahl der ersten Art. Für eine solche Primzahl gilt, weil $f_1(\alpha)$ ebenfalls der ersten Art angehört, nach dem Satze (I.) das Reciprocitätsgesetz:

$$\left(\frac{\phi(\alpha)}{f_1(\alpha)}\right) = \left(\frac{f_1(\alpha)}{\phi_1(\alpha)}\right),$$

man hat also

$$K_1 \equiv K'_1, \quad \text{mod. } \lambda,$$

Aus der Congruenz (18.) fällt daher das zweite Glied hinweg, und dieselbe giebt, wenn durch m dividirt wird, welches den Faktor λ nicht enthält:

$$iK' \equiv i'K, \quad \text{mod. } \lambda, \tag{19.}$$

oder

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right)^i = \left(\frac{\phi(\alpha)}{f(\alpha)}\right)^{i'}. \tag{20.}$$

Es ist nun auch hier zunächst zu ermitteln, in wie weit die Primzahl der ersten Art $\phi(\alpha)$ von den beiden Primzahlen $f(\alpha)$ und $f_1(\alpha)$ unabhängig ist. Dieselbe ist der einzigen Bedingung unterworfen, dafs $\left(\frac{D(\alpha)}{f(\alpha)}\right) = 1$ sein mufs, welche, da $\phi(\alpha)$ eine Primzahl der ersten Art ist, durch passende Wahl der in $D(\alpha)$ enthaltenen beliebigen Einheit $e(\alpha)\, e_1(\alpha)$ immer erfüllt werden kann, wenn nicht, ebenso wie in dem obigen ersten Falle, die Bedingung, dafs $D(\alpha) - 1$ nicht durch ϱ^2 theilbar sein darf, eine Ausnahme begründet. Dieses kann nur dann der Fall sein, wenn $\phi(\alpha)$ die ganz besondere Eigenschaft hat, dafs alle aus den zweigliedrigen Perioden gebildeten Einheiten λte Potenzreste von $\phi(\alpha)$ sind, die Einheit α aber Nichtrest ist, und wenn aufserdem

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right)^m \cdot \left(\frac{f_1(\alpha)}{\phi(\alpha)}\right)^{m'} = 1 \tag{21.}$$

ist. Weil ferner die Zahlen m und m_1 nur in so weit bestimmt sind, dafs sie nicht durch λ theilbar sein dürfen und dafs $f(\alpha)^m$ und $f_1(\alpha)^{m_1}$ wirkliche complexe Zahlen sein sollen, so kann man anstatt m auch km setzen, wo k eine jede der Zahlen $1, 2, 3, \ldots \lambda - 1$ vorstellt. Hieraus folgt, dafs man die Zahlen m und m_1 immer so wählen kann, dafs die Gleichung (21.) nicht Statt hat, ausgenommen in dem Falle, dafs $\left(\frac{f(\alpha)}{\phi(\alpha)}\right)$ und $\left(\frac{f_1(\alpha)}{\phi(\alpha)}\right)$ beide einzeln den Werth Eins haben. Die Primzahl der ersten Art $\phi(\alpha)$ kann also in der Gleichung (20.) namentlich alle diejenigen Werthe ohne Ausnahme erhalten, für welche $\left(\frac{f(\alpha)}{\phi(\alpha)}\right)$ nicht gleich Eins ist, und es wird hinreichen, diese allein in Betracht zu ziehen.

Die erste Folgerung, welche ich aus der Gleichung (20.) ziehe, ist die, dafs, wenn $\left(\frac{f(\alpha)}{\phi(\alpha)}\right)$ nicht gleich Eins ist, i' nicht congruent Null sein kann; da nämlich nach der Voraussetzung i nicht congruent Null ist, so ist auch $\left(\frac{f(\alpha)}{\phi(\alpha)}\right)^i$ nicht gleich Eins und darum i' nicht congruent Null. Also wenn $f_1(\alpha)$ Nichtrest von $f(\alpha)$ ist, so ist auch $f(\alpha)$ Nichtrest von $f_1(\alpha)$. Die Gültigkeit dieses Schlusses hängt jedoch davon ab, dafs man immer eine Primzahl $\phi(\alpha)$ der ersten Art finden kann, für welche eine beliebig gegebene Primzahl $f(\alpha)$ der zweiten Art Nichtrest ist, welches Postulat demjenigen vollständig analog ist, dafs zu jeder gegebenen Primzahl der Form $4n+1$, eine Primzahl der Form $4n+3$ gefunden werden kann, in Beziehung auf welche jene quadratischer Nichtrest ist, welches Legendre in seinem Beweise des quadratischen Reciprocitätsgesetzes gemacht und unbewiesen gelassen hat. Aus dem im §. 16. bewiesenen Satze (I.) folgt aber fast unmittelbar, dafs es stets unendlich viele Primzahlen $\phi(\alpha)$ giebt, welche dieser Forderung genügen. Betrachtet man nämlich in diesem Satze nur zwei gegebene, wirkliche complexe Zahlen, und nimmt für die eine eine Einheit $E(\alpha)$, für die andere aber $f(\alpha)^m$, so zeigt derselbe, dafs es unendlich viele Primzahlen $\phi(\alpha)$ von der Art giebt, dafs

$$\left(\frac{E(\alpha)}{\phi(\alpha)}\right)^k = \alpha^c, \qquad \left(\frac{f(\alpha)}{\phi(\alpha)}\right)^{mk} = \alpha^{c_1}$$

ist, wo c und c_1 beliebig gegebene Zahlen sind, und k nicht durch λ theilbar. Wählt man also c und ebenso auch c_1 nicht durch λ theilbar, so ist $\left(\frac{E(\alpha)}{\phi(\alpha)}\right)$ nicht gleich Eins, also $\phi(\alpha)$ eine Primzahl der ersten Art, und auch $\left(\frac{f(\alpha)}{\phi(\alpha)}\right)$ nicht gleich Eins, wodurch die Existenz unendlich vieler, der Forderung entsprechender Primzahlen bewiesen ist. Die somit streng bewiesene Folgerung: wenn eine Primzahl der ersten Art Nichtrest einer Primzahl der zweiten Art ist, so ist auch diese Nichtrest von jener, bildet die Ergänzung des Satzes (II.) und giebt folgenden vollständigeren Satz:

(III.) Wenn von zwei primären complexen Primzahlen, deren eine der ersten, die andere der zweiten Art angehört, die eine λter Potenzrest der andern ist, so ist auch diese λter Potenzrest von jener.

Um nun für den gegenwärtigen Fall, wo die eine der beiden zu vergleichenden Zahlen der ersten Art angehört, die andere aber der zweiten Art, das Reciprocitätsgesetz auch für die $\lambda-1$ verschiedenen Klassen der Nichtreste in derselben einfachen Form zu erhalten wie im ersten Falle, zeige ich, dafs in der Gleichung (20.) nothwendig $i=i'$ sein mufs. Zu diesem Zwecke wende ich die eine Reciprocitätsgleichung an, welche die Kreistheilung gewährt, nämlich folgende:

$$(22.)\quad \left(\frac{\phi(\alpha)}{f(\alpha)}\right)\cdot\left(\frac{\phi(\alpha)}{f(\alpha^{\gamma})}\right)\cdots\left(\frac{\phi(\alpha)}{f(\alpha^{\gamma^{e-1}})}\right)=\left(\frac{f(\alpha)}{\phi(\alpha)}\right)\cdot\left(\frac{f(\alpha^{\gamma})}{\phi(\alpha)}\right)\cdots\left(\frac{f(\alpha^{\gamma^{e-1}})}{\phi(\alpha)}\right),$$

in welcher $\phi(\alpha)$ ein complexer Primfaktor der Primzahl p von der Form $n\lambda+1$ ist, $f(\alpha)$ ein complexer Primfaktor der Primzahl q, welche zum Exponenten f gehört, nach dem Modul λ, $ef=\lambda-1$ und γ eine primitive Wurzel von λ, so dafs $f(\alpha)$, $f(\alpha^{\gamma})\ldots f(\alpha^{\gamma^{e-1}})$ die e verschiedenen idealen Primfaktoren des q sind. Man sehe die Abhandlung von Eisenstein in den Monatsberichten der Akademie vom Mai 1850.

Ich wähle nun die Primzahl $\phi(\alpha)$ in der Gleichung (22.) so, dafs die $e-1$ zu $f(\alpha)$ conjugirten Zahlen $f(\alpha^{\gamma})$, $f(\alpha^{\gamma^2})$, $\ldots f(\alpha^{\gamma^{e-1}})$ λte Potenzreste für $\phi(\alpha)$ sind, die Zahl $f(\alpha)$ selbst aber ein Nichtrest von $\phi(\alpha)$. Dafs es stets Primzahlen $\phi(\alpha)$ giebt, welche diesen Bedingungen genügen, folgt unmittelbar aus dem Satze (I.) §. 16., wenn in demselben für $F(\alpha)$, $F_1(\alpha)$, $\ldots$ die e wirklichen complexen Zahlen $f(\alpha)^h$, $f(\alpha^{\gamma})^h$, $\ldots$ $f(\alpha^{\gamma^{e-1}})^h$ und irgend eine Einheit $E(\alpha)$ genommen, und die Zahlen, welchen die Indices derselben proportional sein sollen, mit Ausschlufs des Index von $f(\alpha)$ und des Index der Einheit $E(\alpha)$ alle gleich Null gewählt werden. Wenn die Primzahl $\phi(\alpha)$ in dieser Weise bestimmt ist, so erfüllt sie die eine Bedingung: dafs die Norm derselben eine nichtcomplexe Primzahl p von der Form $n\lambda+1$ sei, von selbst; denn die nichtcomplexe Zahl $q=f(\alpha)f(\alpha^{\gamma})\ldots\ldots f(\alpha^{\gamma^{e-1}})$ ist ein Nichtrest von $\phi(\alpha)$ und eine nichtcomplexe Zahl kann nur für solche complexe Primzahlen Nichtrest sein, welche zum Exponenten Eins gehören, das heifst deren Normen Primzahlen der Form $n\lambda+1$ sind.

Wenn nun die complexen Primzahlen $f(\alpha^{\gamma})$, $f(\alpha^{\gamma^2})\ldots f(\alpha^{\gamma^{e-1}})$ λte Potenzreste von $\phi(\alpha)$ sind, so ist nach dem Satze (III.) auch umgekehrt $\phi(\alpha)$ ein λter Potenzrest für jene, und die Gleichung (22.) giebt, wenn für die

Legendreschen Zeichen, deren Werth gleich Eins ist, dieser Werth gesetzt wird:

$$(23.)\qquad \left(\frac{\phi(\alpha)}{f(\alpha)}\right) = \left(\frac{f(\alpha)}{\phi(\alpha)}\right).$$

Für eine solche speciell bestimmte Primzahl $\phi(\alpha)$ ist also in der Gleichung (20.) $i \equiv i'$ und weil i und i' für alle complexen Primzahlen $\phi(\alpha)$ der ersten Art, für welche $f(\alpha)$ ein Nichtrest ist, dieselben Werthe haben müssen, so folgt, dafs für alle diese ebenfalls $i \equiv i'$ oder

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right)^i = \left(\frac{\phi(\alpha)}{f(\alpha)}\right)^i,$$

woraus unmittelbar folgt, dafs auch

$$(24.)\qquad \left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right)$$

ist, wodurch dieses einfache Reciprocitätsgesetz für die verschiedenen $\lambda - 1$ Klassen der Nichtreste bewiesen ist. Da dasselbe nach dem Satze (III.) für die Reste bereits fest steht, so hat man den allgemeineren Satz:

(IV.) Wenn von zwei primären complexen Primzahlen $\phi(\alpha)$ und $f(\alpha)$ die eine der ersten Art, die andere der zweiten Art angehört, so besteht unter denselben das Reciprocitätsgesetz:

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right).$$

Es bleibt nun noch übrig, das Reciprocitätsgesetz auch für den dritten Fall zu entwickeln, wo die zu vergleichenden primären Primzahlen $f(\alpha)$ und $\phi(\alpha)$ beide der zweiten Art angehören. Nimmt man zu diesem Zwecke in der Congruenz (18.) $\phi(\alpha)$ als eine primäre Primzahl der zweiten Art, so hat man, weil das Reciprocitätsgesetz für zwei primäre complexe Primzahlen, deren eine der ersten die andere der zweiten Art angehört, gültig ist:

$$(25.)\qquad \left(\frac{f_1(\alpha)}{f(\alpha)}\right) = \left(\frac{f(\alpha)}{f_1(\alpha)}\right),\quad \left(\frac{f_1(\alpha)}{\phi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f_1(\alpha)}\right),$$

also

$$(26.)\qquad i \equiv i',\qquad K_1 \equiv K_1' \quad \text{mod. } \lambda.$$

Die Congruenz (18.) giebt daher, weil i nicht $\equiv 0$ ist:

$$K' \equiv K,\quad \text{mod. } \lambda,$$

und mithin

$$(27.)\qquad \left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right),$$

welches Resultat für jede complexe Primzahl der zweiten Art $\phi(\alpha)$ gültig ist, die der Bedingung $\left(\frac{D(\alpha)}{\phi(\alpha)}\right) = 1$ genügt. Diese Bedingung giebt, weil in Beziehung auf $\phi(\alpha)$ als Primzahl der zweiten Art jede Einheit ein λter Potenzrest ist:

$$(28.)\qquad \left(\frac{f(\alpha)}{\phi(\alpha)}\right)^{m} \left(\frac{f_1(\alpha)}{\phi(\alpha)}\right)^{m_1} = 1,$$

welcher man durch passende Wahl der Zahlen m und m_1 immer genügen kann, wenn keines der beiden Zeichen $\left(\frac{f(\alpha)}{\phi(\alpha)}\right)$ und $\left(\frac{f_1(\alpha)}{\phi(\alpha)}\right)$ den Werth Eins hat. Wenn man also die Primzahl der ersten Art $f_1(\alpha)$ so wählt, dafs $\left(\frac{f_1(\alpha)}{\phi(\alpha)}\right)$ nicht gleich Eins ist, und dafs auch $\left(\frac{f_1(\alpha)}{f(\alpha)}\right)$ nicht gleich Eins ist, so gilt unter den beiden Primzahlen der zweiten Art $f(\alpha)$ und $\phi(\alpha)$ das Reciprocitätsgesetz (27.) für den Fall, dafs die eine Nichtrest der andern ist; wenn dasselbe aber für die Nichtreste besteht, so folgt von selbst, dafs es auch gelten mufs, wenn die eine Primzahl Rest der andern ist. Es bleibt also nur noch zu zeigen, dafs man, wie auch die beiden Primzahlen der zweiten Art $f(\alpha)$ und $\phi(\alpha)$ gegeben sein mögen, stets eine Primzahl der ersten Art finden kann, welche Nichtrest von $f(\alpha)$ und auch Nichtrest von $\phi(\alpha)$ ist. Wählt man in dem Satze (I.) §. 16. für $F(\alpha)$, $F_1(\alpha)$ ... die wirklichen complexen Zahlen $f(\alpha)^h$, $\phi(\alpha)^h$ und eine Einheit $E(\alpha)$, so zeigt derselbe unmittelbar, dafs es Primzahlen der ersten Art $f_1(\alpha)$ giebt, für welche $f(\alpha)$ und $\phi(\alpha)$ Nichtreste sind, und hieraus folgt nach dem Satze (IV.), dafs auch umgekehrt diese Zahlen $f_1(\alpha)$ sowohl für $f(\alpha)$, als auch für $\phi(\alpha)$ Nichtreste sind. Somit ist die Gültigkeit des einfachen Reciprocitätsgesetzes auch für je zwei Primzahlen der zweiten Art bewiesen, und man hat den Satz:

(V.) Wenn zwei primäre complexe Primzahlen $f(\alpha)$ und $\phi(\alpha)$ beide der zweiten Art angehören, so besteht unter denselben das Reciprocitätsgesetz:

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right).$$

Es besteht also in allen drei unterschiedenen Fällen: wenn beide Primzahlen der ersten Art angehören, wenn eine der ersten Art, die andere der zweiten Art angehört, und wenn beide der zweiten Art angehören, dasselbe einfache Reciprocitätsgesetz. Das Resultat dieser Untersuchung oder das allgemeine Reciprocitätsgesetz, in so weit es hier streng bewiesen worden ist, kann daher vollständig so ausgesprochen werden:

(VI.) Wenn λ eine ungrade Primzahl ist, welche in keiner der $\frac{\lambda-3}{2}$ ersten Bernoullischen Zahlen als Faktor des Zählers enthalten ist, so findet unter je zwei, aus λten Wurzeln der Einheit gebildeten, wirklichen oder idealen, primären complexen Primzahlen $f(\alpha)$ und $\phi(\alpha)$ das Reciprocitätsgesetz Statt:

$$\left(\frac{f(\alpha)}{\phi(\alpha)}\right) = \left(\frac{\phi(\alpha)}{f(\alpha)}\right);$$

wo da's dem Legendreschen analog gebildete Zeichen der Reste und Nichtreste der λten Potenzen durch folgende Congruenz bestimmt ist:

$$\left(\frac{\phi(\alpha)}{f(\alpha)}\right) \equiv \phi(\alpha)^{\frac{Nf(\alpha)-1}{\lambda}} \equiv \alpha^{\kappa}, \quad \text{mod. } f(\alpha),$$

oder wenn $\phi(\alpha)$ ideal, aber $\phi(\alpha)^k$ wirklich ist, durch die Congruenz:

$$\left(\frac{\phi(\alpha)}{f(\alpha)}\right)^k \equiv (\phi(\alpha)^k)^{\frac{Nf(\alpha)-1}{\lambda}} \equiv \alpha^{k\kappa}, \quad \text{mod. } f(\alpha),$$

und wo die Bedingung, dafs eine complexe Zahl $\phi(\alpha)$ primär ist, durch die beiden Congruenzen:

$$\phi(\alpha)\,\phi(\alpha^{-1}) \equiv \phi(1)^2, \text{ mod. } \lambda,$$
$$\phi(\alpha) \equiv \phi(1), \text{ mod. } \varrho^2,$$

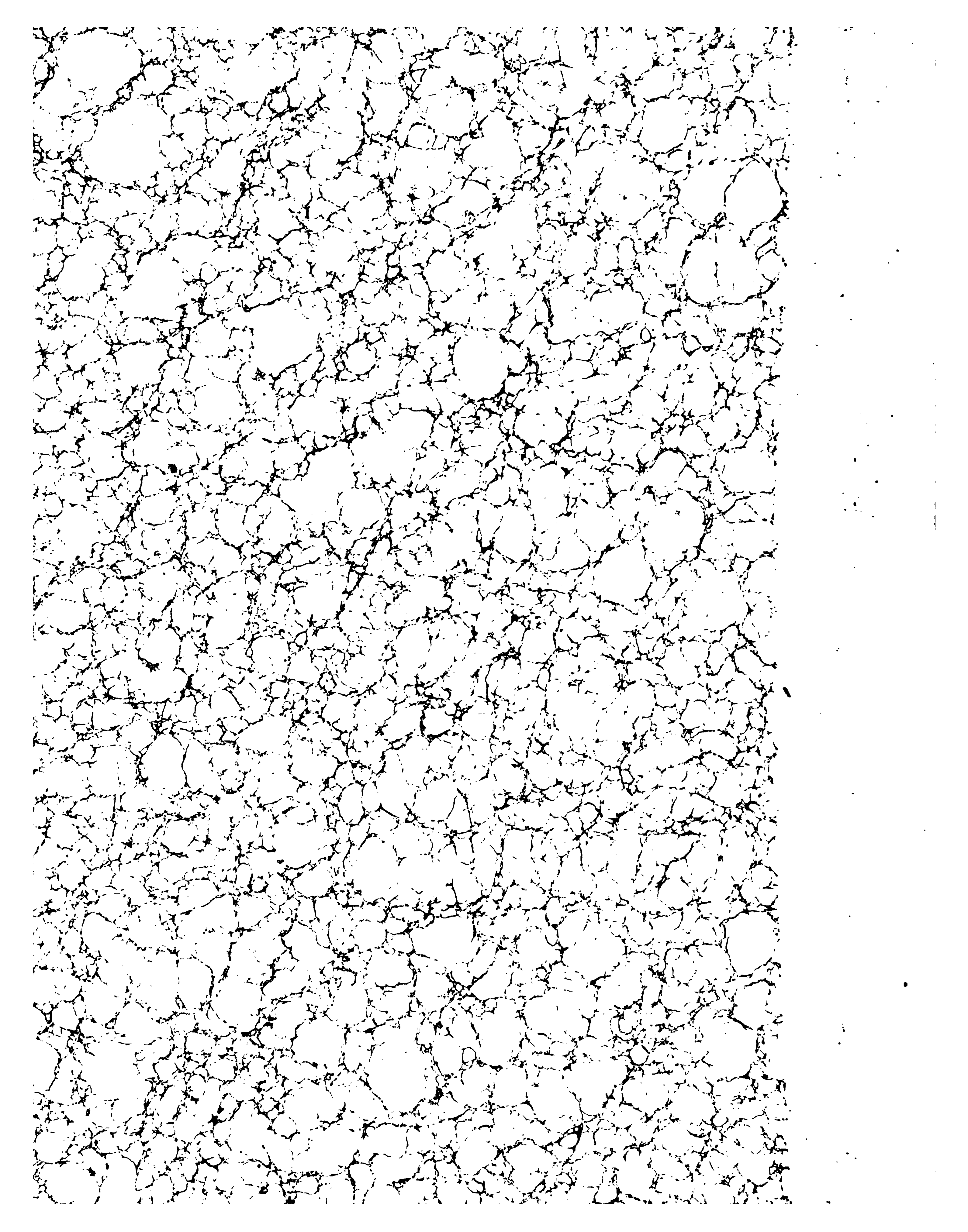
oder wenn $\phi(\alpha)$ ideal, aber $\phi(\alpha)^k$ wirklich ist, durch die Congruenzen:

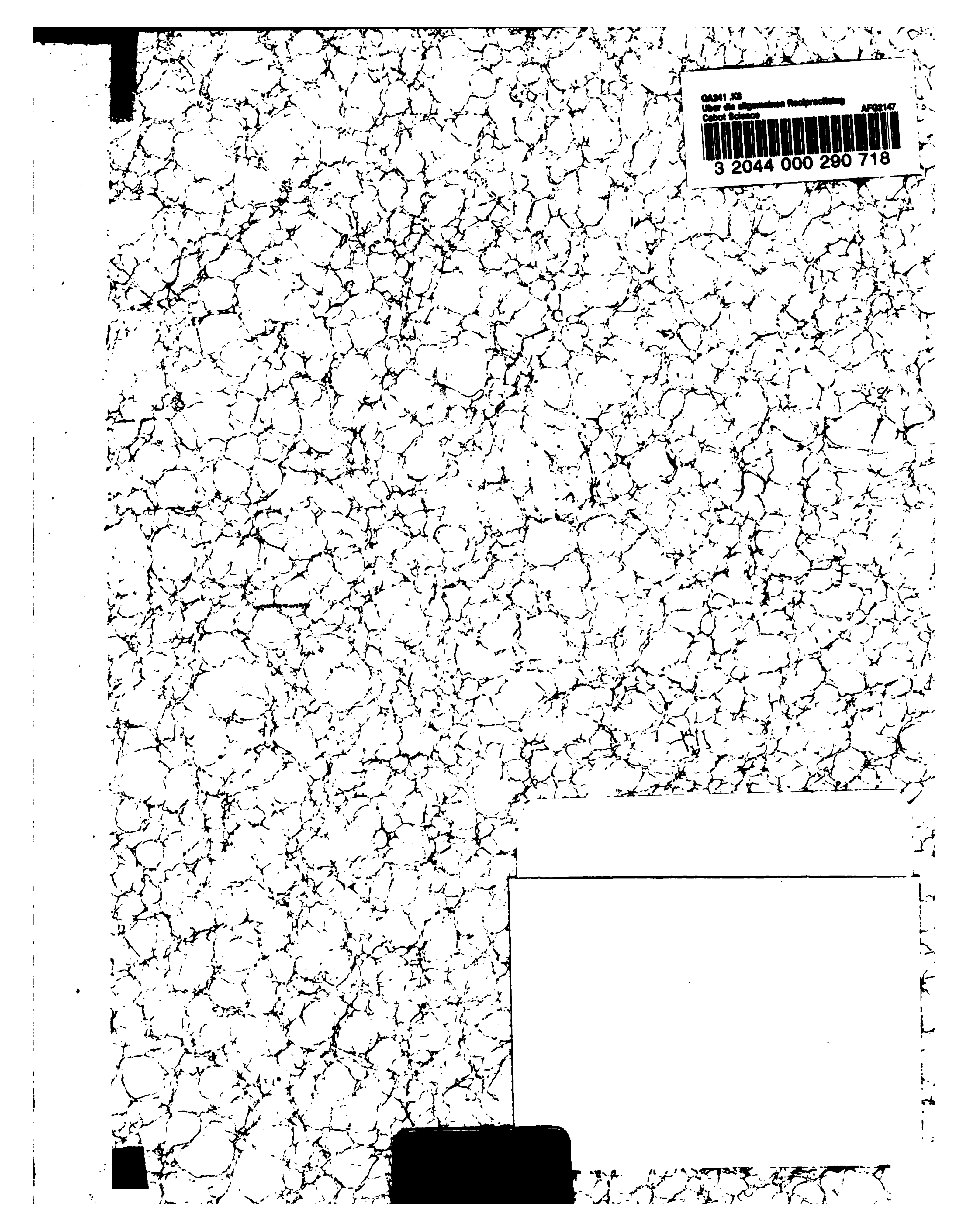
$$\phi(\alpha)^k\,\phi(\alpha^{-1})^k \equiv (\phi(1)^k)^2, \text{ mod. } \lambda,$$
$$\phi(\alpha)^k \equiv \phi(1)^k, \text{ mod. } \varrho^2,$$

bestimmt ist.

Schliefslich bemerke ich, dafs ich aufser dem hier gegebenen Beweise noch zwei andere Beweise des allgemeinen Reciprocitätsgesetzes gefunden habe, welche insofern einfacher sind, als sie bedeutend weniger Vorarbeiten erfordern. Dieselben stützen sich nämlich auf die Theorie der complexen Zahlen in w allein, so dafs die ganze Theorie der complexen Zahlen in z, die Eintheilung der idealen Zahlen dieser Theorie in die Klassen und Gattungen, die ganze Lehre von den ambigen Klassen und die schwierige Bestimmung der Anzahl der wirklich vorhandenen Gattungen erspart wird. Ich habe aber den hier gegebenen Beweis, auch nachdem ich die beiden kürzeren gefunden hatte, nicht unterdrücken wollen, weil er die allgemeine Anwendbarkeit der Principien des entsprechenden Gaufsischen Beweises für die quadratischen Reste ins Licht stellt, und weil er, wenn die nöthigen Sätze aus der Theorie der complexen Zahlen in z einmal entwickelt sind, eben so einfach ist, als diese beiden neuen Beweise, welche ich der Königlichen Akademie bei einer anderen Gelegenheit vorzutragen gedenke.

Inhaltsverzeichnifs.




QA341 .K8
Uber die allgemeinen Reciprocitatsg
AFG2147
Cabot Science
3 2044 000 290 718


QA241 .K8
Uber die allgemeinen Reciprocitatsg
Cabot Science
AFG2147
3 2044 000 290 718